SITZUNGSBERICHTE

LEIBNIZ-SOZIETÄT DER WISSENSCHAFTEN

Technik – Sicherheit – Techniksicherheit

5. Symposium des Arbeitskreises Allgemeine Technologie der Leibniz-Sozietät der Wissenschaften zu Berlin und des Instituts für Technikfolgenabschätzung und Systemanalyse des Karlsruher Instituts für Technologie am 16. November 2012 in Berlin

Herausgegeben von Gerhard Banse & Ernst-Otto Reher

Mit Beiträgen von Dietrich Balzer, Gerhard Banse, Lucia Belyová, Martin Endreß, Wolfgang Fratzscher, Mukayil Kilic, Klaus Fuchs-Kittowski, Christian Kohlert, Norbert Mertzsch, Benjamin Rampp, Ernst-Otto-Reher, Annely Rothkegel, Dieter Seeliger

BAND 116

JAHRGANG 2013

Inhalt

Gerhard Banse
Geleitwort 5

Gerhard Banse, Ernst-Otto Reher
Einleitung 9

Lucia Belyová, Gerhard Banse
Sicherheit und Sicherheitskultur 21

Wolfgang Fratzscher
Über die Sicherheitskultur bei Kernkraftwerken 33

Norbert Mertzsch
Sicherheitsaspekte beim Rückbau des KKW Rheinsberg 51

Dieter Seeliger
Fukushima – bisherige Lehren aus der Katastrophe über die Sicherheit von Kernkraftwerken 59

Ernst-Otto Reher
Überwachung und Qualitätssicherung fluider, strukturierter Erzeugnisse aus Produktionsanlagen, dargestellt am Beispiel der Kunststofftechnologie 79

Christian Kohlert
Sicherheit gegen Produktfälschung 99

Dietrich Balzer
Die gegenwärtige und zukünftige Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft 111

Mukayil Kilic, Klaus Fuchs-Kittowski
Sicherheitsrisiken und Vermeidungsverhalten im Fall der modernisierten und neuen Informationsquellen bei der Lenkung und Remotefunktionen von Fahrzeugen – Zusammenfassung 123

Annely Rothkegel
Sicherheitskommunikation: Kommunikationskulturen im Kontext der Techniknutzung 125

Martin Endreß, Benjamin Rampp
Vertrauen in der Sicherheitsgesellschaft 145

Ernst-Otto Reher, Gerhard Banse
Schlusswort 161

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 5–7*

Gerhard Banse

Eröffnung

Meine sehr geehrten Damen und Herren,

ich begrüße Sie im Namen der Veranstalter – der Leibniz-Sozietät der Wissenschaften zu Berlin und ihres Arbeitskreise „Allgemeine Technologie“ sowie des Instituts für Technikfolgenabschätzung und Systemanalyse des Karlsruher Instituts für Technologie – ganz herzlich zum Symposium „Technik – Sicherheit – Techniksicherheit“.

Dieses Symposium ist das fünfte seiner Art, initiiert und organisiert in den zurückliegenden 11 Jahren durch den Arbeitskreis „Allgemeine Technologie“. Waren die ersten drei eher inhaltlich-konzeptionellen Aspekten der Allgemeinen Technologie im engeren Sinne gewidmet:

- Allgemeine Technologie – Vergangenheit, Gegenwart, Zukunft (2001),
- Fortschritte bei der Herausbildung der Allgemeinen Technologie (2004) und
- Allgemeine Technologie – verallgemeinertes Fachwissen und konkretisiertes Orientierungswissen zur Technologie,

so wandte sich das 4. Symposium im Jahre 2010 mit „Ambivalenzen von Technologien – Chancen, Gefahren, Missbrauch“ einer *gesellschaftlich* relevanteren Thematik zu. Das diesjährige und 5. Symposium nun hat eine zentrale Thematik zum Gegenstand: „Sicherheit“. Zunächst abgesehen davon, dass „Sicherheit“ ein schillernder, facettenreicher und ubiquitär verwendeter Begriff ist: Generell wird damit ein Zustand der Gewissheit, der Zuverlässigkeit und des Unbedrohtseins erfasst (auch wenn das stets nur „relativ“ ist). Und: Ungewissheiten, Unzuverlässigkeiten sowie Bedrohungen gibt es zahlreich(e) – auch oder gerade im Zusammenhang mit technischen Hervorbringungen. Lassen Sie mich nur zwei Ereignisse nennen, wobei das zweite heute noch mehrfach Gegenstand der Betrachtung sein wird:

1. Am 14. April 1912 – also vor gut 100 Jahren – kollidierte auf „ihrer Jungfernfahrt […] die *Titanic* gegen 23:40 Uhr etwa 300 Seemeilen südöstlich

von Neufundland seitlich mit einem Eisberg und sank zwei Stunden und 40 Minuten nach dem Zusammenstoß im Nordatlantik. Obwohl für die Evakuierung mehr als zwei Stunden Zeit zur Verfügung standen, starben zwischen 1490 und 1517 der über 2200 an Bord befindlichen Personen – hauptsächlich wegen der unzureichenden Zahl an Rettungsbooten und der *Unerfahrenheit der Besatzung* [H.d.V.; G.B.] im Umgang mit diesen. Wegen der hohen Opferzahl zählt der Untergang der *Titanic* zu den großen Katastrophen der Seefahrt.“[1]

2. Am 11. März 2011 um 14:47 Uhr (Ortszeit) kam es im Zusammenhang mit dem Tōhoku-Erdbeben kam es zu schweren Störfällen in vier von sechs Reaktorblöcken des japanischen Kernkraftwerks Fukushima Daiichi: „In Block 1 bis 3 kam es zu Kernschmelzen. Große Mengen an radioaktivem Material […] wurden freigesetzt und kontaminierten Luft, Böden, Wasser und Nahrungsmittel in der land- und meerseitigen Umgebung. Ungefähr 100.000 bis 150.000 Einwohner mussten das Gebiet vorübergehend oder dauerhaft verlassen. Hunderttausende in landwirtschaftlichen Betrieben zurückgelassene Tiere verendeten.“[2]

Allein die öffentliche Diskussion und mediale Reaktion auf diese beiden katastrophalen Ereignisse machen deutlich, dass die Sicherheit technischer Handlungsvollzüge und technischer Hervorbringungen als weitgehender Ausschluss oder als bewusstes Handling von Risiken in den handlungsleitenden Wertvorstellungen technischer Welterzeugung einen herausragenden Platz einnimmt.

Mehr noch: Sicherheit ist ein zentrales Konzept in Gesellschaft, Wissenschaft und Technik. In einer mir gerade zugesandten Broschüre des BMBF heißt es deshalb (vor dem Hintergrund des BMBF-Rahmenprogramms „Zivile Sicherheit“) auch: „Ein wichtiges Ziel des neuen Rahmenprogramms besteht darin, die Bevölkerung auch zukünftig adäquat auf den Umgang mit Risiken vorzubereiten und in akuten Katastrophenfällen wirksam und umfassend zu schützen. Auf dem BMBF-Innovationsforum wurden daher auch die gesellschaftlichen Aspekte der zivilen Sicherheitsforschung eingehend erörtert. Zentrale Fragestellungen dazu lauteten: Welche Lösungen eignen sich für die Erhöhung der zivilen Sicherheit in einer offenen und demokratischen Gesellschaft? Wie kann die Risikokommunikation für die Prävention und Bewältigung von Katastrophen ausgebaut werden? Welche Rolle spielen dabei

1 http://de.wikipedia.org/wiki/RMS_Titanic.
2 http://de.wikipedia.org/wiki/Nuklearkatastrophe_von_Fukushima.

die alten und die neuen Medien, wie etwa Soziale Netzwerke im Internet? Wie können Schutzziele definiert werden und wie geht eine Gesellschaft, in der bereits hohe Sicherheitsstandards existieren, mit Restrisiken um?“ (BMBF 2012, S. 3).

Geprägt wird das Konzept „Sicherheit“ nicht nur von unterschiedlichen Begriffsauffassungen, Kommunikationsstrategien und kulturellen Aspekten, sondern es stellt auch ein inter- und transdisziplinäres Forschungsfeld dar (vgl. Banse et al. 2009). Deshalb hatte ich in meiner Rede auf dem Leibniztag 2012 im Zusammenhang mit möglichen zukünftigen Arbeitsfeldern der Leibniz-Sozietät auch ausgeführt: „Trotz – oder gerade – wegen dieser Ubiquität von Sicherheit bietet sich hier eine Thematik an, die hinsichtlich Wahrnehmung, Bewertung, Kommunikation und Management sicherheitsbeeinflussender Bedingungen und Mechanismen Interdisziplinarität geradezu herausfordert, geht es doch gleichermaßen um kognitive, normative und prozedurale, um deskriptive wie präskriptive Statements“ (Banse 2012, S. 33).

In dem heutigen Symposium werden (auch) deshalb Wissenschaftler aus verschiedenen Disziplinen (sowohl der Natur- und Technik- als auch der Sozial- und Geisteswissenschaften) ihre Forschungsergebnisse zum Thema (Technik-)Sicherheit mit dem Ziel diskutieren, gemeinsame Forschungsansätze vor allem zu „direkter“ Techniksicherheit, aber auch zu Sicherheitskommunikation und Sicherheitskulturen zu entwickeln.

Ich bedanke mich schon jetzt – „vorab“ – sowohl bei den Initiatoren und Organisatoren dieses Symposiums – vor allem bei Ernst-Otto Reher und Heinz-Jürgen Rothe von der Leibniz-Sozietät sowie Bettina-Schmidt-Leis vom ITAS in Karlsruhe – als auch bei der Rosa-Luxemburg-Stiftung, die das Symposium finanziell unterstützt.

Literatur

Banse, G. (2012): Bericht des Präsidenten an den Leibniztag 2012. In: Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 114, S. 9-34

Banse, G.; Rothkegel, A.; Renn, O. (2009): Interdisziplinäre Sicherheits- und Risikoforschung. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 155-170

BMBF (Hg.): BMBF-Innovationsforum „Zivile Sicherheit“. Sicherheit in einer offenen Gesellschaft. Konferenzergebnisse vom 17. bis 19. April 2012, Berlin. Bonn 2012 (auch unter http://www.bmbf.de/pub/innovationsforum_zivile_sicherheit_2012.pdf verfügbar)

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 9–20*

Gerhard Banse, Ernst-Otto Reher

Einleitung

Der Arbeitskreis „Allgemeine Technologie“ der Leibniz-Sozietät der Wissenschaften[1] führte am 16. November 2012 sein V. Symposium zur Thematik „Technik – Sicherheit – Techniksicherheit“ durch.[2]

Die Komplexität des Gegenstandes „Sicherheit“ wird in der nachfolgenden Abbildung 1 verdeutlicht. Um zu einem gesellschaftlichen Handlungsalgorithmus in Fragen der Sicherheit zu gelangen, sind vielfältige Sichten und Handlungen aus Wissenschaft, Wirtschaft, Kultur, Öffentlichkeit und Politik möglich bzw. erforderlich. Erst durch eine breit angelegte Betrachtung können Entscheidungsträger wirksam werden, das betrifft sowohl die Ebene der Artefakte mit ihren Produkten, als auch die menschliche Gesellschaft mit ihrer Umwelt, ihrem Lebensraum von Mensch, Tier und Pflanzen. Das „in die Welt setzen“ von Artefakten und Erzeugnissen von Produktions- und Dienstleistungstechnologien bedarf mehr denn je in unserer Zeit einer kritischen Sicherheitsbetrachtung. Eine Vielzahl von Maßnahmen, in Abbildung 1 nur auszugsweise dargestellt, wurde bisher entwickelt und konnten zum Einsatz gebracht werden (z.B. Technologiefolgenabschätzung, Begleitforschung).

Das Symposium behandelte Aspekte der Technologie- und Erzeugnissicherheit mit den Komplexen „Maschinen-, Apparate- und Anlagensicherheit“, „Erzeugnis- und Produktsicherheit“, „Sicherheit von Dienstleistungstechnologien“ und „Verbrauchersicherheit“.

Sicherheit ist ein zentrales Konzept in Gesellschaft, Wissenschaft und Technik. Geprägt wird dieses Konzept von unterschiedlichen Begriffsauffassungen, Kommunikationsstrategien und kulturellen Aspekten. In dem eintägigen Symposium haben Wissenschaftler aus verschiedenen Disziplinen ihre

1 Vgl. zum Arbeitskreis http://www.leibniz-sozietaet.de/ → Sozietät → Arbeitskreise → Arbeitskreis Allgemeine Technologie.

2 Die vier vorangegangenen Symposien zur Allgemeinen Technologie sind in den Bänden 50, 75, 99 und 112 der Sitzungsberichte der Leibniz-Sozietät dokumentiert (vgl. Banse/Reher 2002, 2004, 2008, 2011).

Forschungsergebnisse zum Thema (Technik-)Sicherheit mit dem Ziel diskutiert, gemeinsame Forschungsansätze vor allem zu Techniksicherheit, aber auch zu Sicherheitskommunikation und Sicherheitskulturen zu entwickeln.[3]

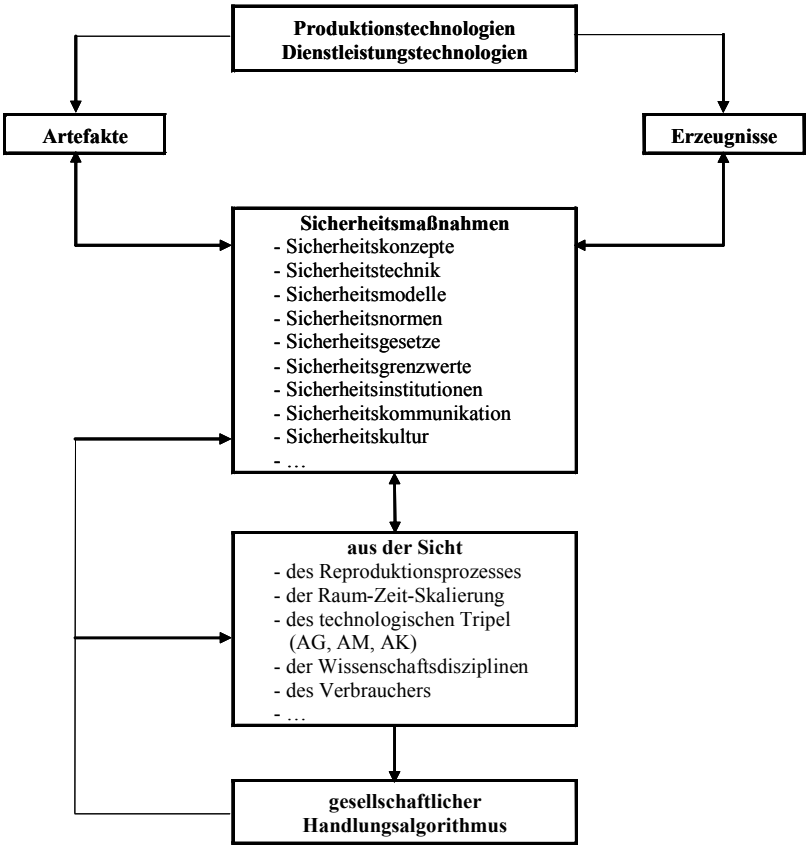


Abbildung 1: Sicherheitsmaßnahmen
Eigene Darstellung

Die Sicherheit technischer Handlungsvollzüge und technischer Hervorbringungen als weitgehender Ausschluss oder als bewusstes Handling von Risiken nimmt in den handlungsleitenden Wertvorstellungen technischer

3 Vgl. zu Techniksicherheit generell z.B. Banse 2013; Banse et al. 2009; Meyna/Peters 1985/86; Perrow 1987; Poy et al. 1994; Schneider 1991; Winzer et al. 2009.

Welterzeugung einen herausragenden Platz ein (vgl. näher dazu Banse 2009, 2011; Belyová/Banse 2011).

Als „Wissenschaften vom Machen“ sind zunächst die Technikwissenschaften herausgefordert, Sicherheit „zu erzeugen“, d.h. technische Sachsysteme und Technik-Mensch-Interaktionen so zu entwerfen und zu gestalten, dass von ihnen (ideal) keine bzw. (real) nur geringe Gefährdungen für „Schutzgüter“ ausgehen (nicht nur aktuell, sondern auch langfristig). Doch sind heute auch die Geistes- und Sozialwissenschaften aufgefordert, sich mit technikbezogener Sicherheit zu befassen, da technische Sachsysteme und Technik-Mensch-Interaktionen in einen sozialen und kulturellen Kontext eingebettet sind. Damit wächst die Relevanz der interkulturellen Forschung unter dem Einfluss der zunehmenden Globalisierung von Technikentwicklung und -anwendung (vgl. z.B. Gronau/Eversheim 2008; Hermeking 2010; Rösch 2008).

*****

Lucia Belyová und *Gerhard Banse* gehen in ihrem Beitrag „Sicherheit und Sicherheitskultur“ davon aus, dass „Sicherheit“ einerseits ein zentraler Gegenstand wissenschaftlicher Forschung, andererseits ein schillernder Begriff ist, mit zahlreichen unterschiedlichen Bedeutungen belegt. Die Sicherheit in Mensch-Technik-Interaktionen lässt sich erhöhen

- durch „Investitionen“ in die technischen Sachsysteme bei deren konstruktiver Auslegung und produktionstechnischer Herstellung (etwa durch Verbesserungen hinsichtlich Zuverlässigkeit und Handhabbarkeit, der Schadensvorbeugung und der Gefährdungsabwehr);
- durch „Investitionen“ in die „Nutzer“ technischer Sachsysteme (etwa durch die Ausprägung von Kompetenz und spezifischer Persönlichkeitseigenschaften);
- durch „Investitionen“ in das (rechtliche, soziale, kulturelle, …) „Umfeld“ der Technikherstellung, vor allem aber der Techniknutzung.

Dieses „Umfeld“ wird weitgehend (jedoch nicht vollständig!) durch das geprägt, was man seit etwa drei Jahrzehnten als „Sicherheitskultur“ bezeichnet. Damit wird eine Einsicht thematisiert, die spätestens mit der Reaktorkatastrophe von Chernobyl im Jahre 1986 gewonnen wurde: neben technischen und unmittelbar an den Nutzer adressierte Maßnahmen sind sozio-kulturelle Aspekte von entscheidender Bedeutung für die Sicherheit von bzw. in Technik-Mensch-Interaktionen. Darauf wird im Beitrag eingegangen. Das Konzept

„Sicherheitskultur“ wird genutzt, um kulturbedingte Verhaltensmerkmale zu beschreiben, die für die Gewährleistung der technikbezogenen Sicherheit („Techniksicherheit“) im komplexen Zusammenspiel von Technik, Organisation, Mensch und Umwelt für von Bedeutung sind.

Sicherheitskultur(en) besitzen einerseits eine mehr „theoretische bzw. normative“ Ebene (vor allem in Form von Anweisungen, Regeln, Vorschriften, Statements, Codes usw.; „externe Ebene“), andererseits eine mehr „praktische bzw. faktische“ Ebene (als gelebte und praktizierte Sicherheitskultur; „interne Ebene“). Letztere erfasst die Einstellungen und das Verhalten (vor allem) von Techniknutzern sowie die Kommunikation zwischen ihnen. Sicherheitskulturen bieten für den einzelnen Nutzer einen Rahmen, der die Ordnung menschlicher Wahrnehmung und Wertung sicherheitsrelevanter Sachverhalte und Zusammenhänge einerseits erst ermöglicht, andererseits auch strukturiert. Zugleich gehen in („gelebte“) Sicherheitskultur(en) unreflektierte Denkgewohnheiten und Handlungsprogramme sowie implizite Werthaltungen der Akteure ein. Für Sicherheitskulturen ist bedeutsam, dass nicht alle relevanten Akteure innerhalb einer Sprachgemeinschaft (etwa Konstrukteure und Nutzer) die gleichen unreflektierten und impliziten Werthaltungen besitzen bzw. entsprechend handeln. Das kann schwerwiegende Folgen haben (z.B. sprachliche Missverständnisse oder Übersetzungsfehler als Auslöser von Irrtümern mit Unfallfolgen). Bei Techniktransfer in andere Länder und damit andere Kulturen kommt hinzu, dass einerseits unterschiedliche Sicherheitskulturen (die der Ursprungs- und die der Zielregion) relevant werden, andererseits weitergehende „höherstufige“ sprachliche Verständigungsprozesse erforderlich sind.

Eine Operationalisierung (und damit auch Vergleichbarkeit) von Sicherheitskulturen ist derzeit (noch) schlecht durchführbar, da (inter- wie intrakulturelle) Indikatoren bislang kaum entwickelt wurden. Im Beitrag wird jedoch ein eigener Vorschlag vorgestellt.

An diese Überlegungen, die zugleich den Eröffnungs- bzw. Einleitungsvortrag des Symposiums bildeten, schließen drei inhaltliche Komplexe an: *erstens* Sicherheit im Zusammenhang mit der Kerntechnologie (Beiträge von Wolfgang Fratzscher, Norbert Mertzsch und Dieter Seeliger), *zweitens* Sicherheit und Materialtechnologie (Beiträge von Ernst-Otto Reher, Christian Kohlert und Dietrich Balzer) sowie *drittens* sozial- und geisteswissenschaftlichen Fragestellungen im Zusammenhang mit Sicherheit (Beiträge von Mukayil Kilic/Klaus Fuchs-Kittowski, Annely Rothkegel sowie Martin Endress/ Benjamin Rampp).

Wolfgang Fratzscher schließt mit seinem Beitrag „Über die Sicherheitskultur bei Kernkraftwerken“ unmittelbar an den Einführungsbeitrag an. Einleitend wird ein kurzer Blick auf die Herausbildung des Begriffes Sicherheit geworfen. Dann wird versucht, die wesentlichen Beiträge der Kerntechnik zur Entwicklung einer Sicherheitskultur aufzuzeigen. Dazu dient zunächst eine Sicht auf das Genehmigungsverfahren in Deutschland mit der Gesellschaft für Reaktorsicherheit, das sich herausgebildet hat aufgrund der speziellen Sicherheitsaspekte bei kernenergetischen Anlagen. Es ist dies das Auftreten der radioaktiven Strahlung, die durch Abschirmung und gas- und druckdichte Barrieren zurückgehalten werden soll. Es sind dies weiter die Maßnahmen zur Eindämmung der Auswirkungen menschlichen Fehlverhaltens und die Orientierung der Sicherheitsmaßnahmen am Lebenszyklus der Anlagen einschließlich der möglichen Unfälle bis hin zu Katastrophen und der endgültigen Beseitigung der Anlagen. Weiter wird angenommen werden, dass die Kerntechnik maßgebend zur Herausbildung der Technikfolgenabschätzung (TA) beigetragen hat. Diese hat, wie auch die Versuche, die Sicherheitsphilosophie der Kerntechnik auf andere Industriebereiche zu übertragen, nicht den erwarteten Erfolg gebracht. Das beweist, dass das Sicherheitsniveau in der Kerntechnik in manchen Dimensionen höher ist als in anderen Bereichen der Volkswirtschaft. Das schließt aber nicht aus, das außer der Sicherheit alle anderen Bewertungskriterien für die Einschätzung der Kerntechnik nicht mehr maßgebend sind. Abschließend wird eine Struktur der Gesamtheit der Sicherheitsdimensionen auf der Grundlage technologischer Überlegungen entworfen, deren Erfüllung für eine Einschätzung des Niveaus der Sicherheitskultur zugrunde gelegt werden kann.

Norbert Mertzsch behandelt „Sicherheitsaspekte beim Rückbau des KKW Rheinsberg“. Das Thema „Sicherheit“ hat bei der Stilllegung und dem Rückbau des Kernkraftwerkes Rheinsberg absolute Priorität. Dabei rücken entsprechend des Rückbaufortschritts jeweils unterschiedliche Sicherheitsaspekte in den Focus. Bei allen Maßnahmen zur Stilllegung des Kernkraftwerkes Rheinsberg besitzen Strahlenbetrachtungen für das Personal, die Bevölkerung und die Umgebung die entscheidende Bedeutung. Im Rahmen der Arbeitsplanung wurden und werden Maßnahmen zur Gewährleistung des Strahlenschutzes detailliert festgelegt. Durch technische Maßnahmen wird im Kernkraftwerk Rheinsberg sichergestellt, dass die im Rahmen der Stilllegungsgenehmigung festgelegten Grenzwerte für die Abgabe von Radionukliden über die Abluft und das Abwasser während der Stilllegungsarbeiten jederzeit sicher unterschritten werden. Dem physischen Schutz von Kern-

brennstoff wurde in der Nachbetriebsphase höchste Aufmerksamkeit gewidmet. Nach dem Abtransport des Kernbrennstoffs konnten die diesbezüglichen Maßnahmen deutlich reduziert werden, da sich das Gefährdungspotenzial drastisch verringerte. Für die weiteren Stilllegungs- und Rückbauarbeiten ist das Schutzziel „Rückhaltung radioaktiver Stoffe" stets zu gewährleisten.

Ein weiterer wichtiger Sicherheitsaspekt ist die Arbeitssicherheit, denn Demontage- und Abbrucharbeiten gehören zu den Tätigkeiten mit erheblichem Gefährdungspotenzial. Das Gefährdungspotenzial besteht vor allem

- im Umgang mit schweren Lasten;
- durch die räumliche Enge;
- in der Gewährleistung der Statik der Anlagen und Gebäude;
- in der Beseitigung von Gefahrstoffen, wie Asbest;
- durch das Auftreten von Stäuben, radioaktiven Aerosolen, ionisierender Strahlung und Kontaminationen.

Dieser Beitrag kann für weitere KKW-Rückbauvorhaben als Beispiel angesehen und die gewonnenen Erfahrungen von Rheinsberg können sicherlich übernommen werden.

Dieter Seeliger wendet sich „Fukushima – bisherige Lehren aus der Katastrophe über die Sicherheit von Kernkraftwerken" zu. Am 11. März 2011 erschütterte das bisher schwerste Erd- und Seebeben im Pazifik östlich von Japan die Region und löste mehrere Tsunami-Wellen aus, die weite Küstenbereiche im Nordosten der Hauptinsel Honshu überschwemmten und weiträumig totale Zerstörungen an Wohnsiedlungen, Infrastruktur, Industrieanlagen und landwirtschaftlich genutzten Flächen hinterließen. Als schwerster Verlust infolge dieser Naturkatastrophe sind tausende Menschenleben zu beklagen, viele werden noch immer vermisst. In der Kernkraftanlage Fukushima Dai-ichi mit sechs Reaktorblöcken setzten Erdbeben und Seewasser-Überflutung infolge des Tsunami die Reaktorkühlsysteme außer Betrieb, was nachfolgend zu schwersten Zerstörungen an vier Reaktoren und großflächiger Freisetzung von Radioaktivität führte, in deren Ergebnis dieser Reaktorunfall in die höchste Stufe der internationalen Skala eingeordnet wurde. Im Beitrag werden kurz die Abfolge der eingetretenen Zerstörungen und deren Auswirkungen sowie die Einleitung von sofortigen Gegenmaßnahmen und Ausarbeitung von Plänen zur mittel- und langfristigen Sicherung und Dekontaminierung seitens des Kraftwerksbetreibers TEPCO und der japanischen Atomaufsichtsbehörden erläutert.

Parallel zu den Aktivitäten vor Ort starteten internationale Gremien, insbesondere auf Initiative und unter Führung der Internationalen Atombehörde

IAEA der UNO in Wien, zahlreiche Projekte – Expertenmissionen, Konferenzen, Workshops etc. – mit dem Ziel, die Ursachen der Katastrophe und den aktuellen Stand ihrer Überwindung zu erfassen bzw. offen zu legen, notwendige Schlussfolgerungen hinsichtlich der Sicherheit des weiteren Betriebs der weltweit laufenden 430 Kernkraftwerke und Empfehlungen für erhöhte Sicherheitsvorschriften bei der Auslegung von Neuanlagen auszuarbeiten und diese über Beschlüsse der Regierungen in die verbindliche Rechtspraxis der Mitgliedsländer einfließen zu lassen. Hervorgehoben wird in diesem Zusammenhang auch die Durchführung von Stresstests an den KKW in der EU auf Vorschlag und Initiative der westeuropäischen kerntechnischen Genehmigungs- und Aufsichtsbehörde WENRA (Western European Nuclear Regulators‘ Association).

Wie ist der heutige Stand des Reaktorunfalls von Fukushima und sind die Perspektiven der Überwindung seiner Folgen zu bewerten? Wie groß sind mittel- und langfristige Schäden bei Menschen und Tieren infolge der erhöhten Strahlenbelastung zu erwarten? Handelt es sich bei diesem Unfall um das Eintreten eines angeblich „unvermeidlichen Restrisikos“ der komplexen Kernenergie-Technik? Zu diesen und weiteren Fragen versucht der Beitrag – über ein Jahr nach der Katastrophe – vorläufige Antworten zu finden.

Mit diesem Beitrag wird eine Reihe von offenen Fragen beantwortet, die bisher in dieser deutlichen Darstellung in der Öffentlichkeit nicht behandelt wurden. Die eingeleitete Energiewende in Deutschland bekommt so sicherlich weitere Befürworter.

Ernst-Otto Reher behandelt die „Überwachung und Qualitätssicherung fluider strukturierter Erzeugnisse aus Produktionsanlagen, dargestellt am Beispiel der Kunststofftechnologie“. Er kommt zu folgenden generalisierten Aussagen:

1. Produktionsanlagen der Materialtechnologien haben heutzutage eine Produktionskapazität, die Labormessverfahren zur Qualitätssicherung nur in seltenen Fällen zulassen. Zu groß ist der Ausschuss, der in der Prüfzeit im Labor die Anlage verlässt, z.B. 100 t/h Kunststoffe. Es kommen immer mehr online-Messverfahren im Echtzeitbetrieb zum Einsatz, um die Ausschussquote zu verhindern oder wesentlich zu minimieren.
2. Für strukturierte Fluide (Polymerschmelzen und -lösungen, Lebensmittel, Kosmetika, Pharmaka, Bio- und Nanoprodukte, Keramikschlicker, Farben und Lacke, Betonsuspensionen, Beschichtungsmassen u.v.m.) sind die rheologischen Eigenschaften signifikant für Struktur-Eigenschafts-Beziehungen, die die Verarbeitbarkeit dieser Fluide und ihre Anwendung

in der Praxis bestimmen. Auch weitere zusätzliche Messverfahren kommen zum Einsatz, z.B. IR-Spektroskopie.

3. Bei Nichteinhaltung vorgegebener rheologischer Eigenschaften der Polymerschmelzen bei der Synthese sind die Verarbeiter und Anwender der Polymerschmelzen (Granulat) nicht in der Lage, ihre Erzeugnisse in Qualität und Quantität mit ihren Verarbeitungsanlagen herzustellen. Das geforderte „Verarbeitungsfenster" der Anlagen wird durch die rheologischen (strukturellen) Eigenschaften der Polymerschmelzen begrenzt. Die Polymerhersteller müssen die geforderten rheologischen Eigenschaften der Verarbeiter und Anwender garantieren. Ähnlich verhält es sich mit anderen strukturierten fluiden Erzeugnissen.
4. Die rheologischen Prozessgrenzen der Verarbeitungsanlagen im Arbeitsdiagramm können durch mathematische Prozessmodelle der Verarbeitungsausrüstung mit den rheologischen Materialfunktionen vorausberechnet werden. Für sie werden Intervalle zur Verarbeitbarkeit und Produktanwendung angegeben, die der Polymerhersteller garantieren muss. Die Durchsatzsteigerungen sind mit zusätzlichen Kosten verbunden, eine Kostenanalyse ermöglicht eine Technologieentscheidung.
5. Die Entwicklung der Mess- und Steuerverfahren einschließlich der dazu gehörigen Technik wird im Team von Materialwissenschaftlern (Naturwissenschaftlern) und Technikwissenschaftlern für die online-Verfahren betrieben. Sozial- und Geisteswissenschaftler erarbeiten Grenzwerte sowie Normen und sind bei den Gesetzesvorbereitungen involviert (siehe Abbildung 1).
6. Am Beispiel der Kunststofftechnologie werden verschiedene entwickelte Struktur-Eigenschafts-Beziehungen dargestellt, die für die online-Rheometrie im Echtzeitbetrieb entwickelt und angewendet wurden. Die Anwendung der Verfahren und der entwickelten technischen Lösungen konnten auch für andere, oben aufgezählte strukturierte Fluide erweitert und angewendet werden. Somit entstand ein Instrumentarium an Soft- und Hardware zur Überwachung und Qualitätssicherung fluider Erzeugnisse in der Stoffwirtschaft.

Der Ausgangspunkt im Beitrag von *Christian Kohlert* „Sicherheit gegen Produktfälschung" ist die Feststellung, dass Produktfälschungen und Plagiate schon lange keine „Kavaliersdelikte" mehr sind, sondern den Volkswirtschaften sowie den im guten Glauben befindlichen Nutzern erhebliche Schäden zufügen. So werden Forschungsaufwendungen, wie z.B. in der Pharmaindustrie, nicht über das entstandene Produkt finanzierbar gemacht,

und die Endproduktnutzer müssen möglicherweise ohne den angestrebten Nutzeffekt auskommen (bis hin zu persönlichen Schäden durch fehlende oder minderwertige Wirkstoffe). Einer Studie der OECD aus dem Jahre 2009 zufolge belaufen sich die Schäden dieser Produktpiraterie weltweit auf 184 Mrd. Euro und betragen damit schon über 50 Prozent mehr als 2007. Schätzungen gehen davon aus, dass dadurch alleine in Deutschland jährlich rund 50.000 Stellen verloren gehen. Selbstverständlich sind bestimmte Produktgruppen, wie hochwertige Konsumgüter der Bekleidungsindustrie, Kosmetika und Pharmazeutika, vorrangig betroffen, aber ausgespart vor diesem Problem ist fast keine Branche mehr.

Bei Plagiaten geht es in der Regel darum, unter hochwertigen Markennamen minderwertige Produkte zu verkaufen. Durch Kopieren der notwendigen Maschinen und Anlagen, durch Nutzung minderwertiger Rohstoffe sowie durch Umgehung qualitätssichernder Maßnahmen werden enorme Gewinnspannen erzielt. Da die Produkte selbst oft schwer prüfbar sind, wird in letzter Zeit verstärkt die Verpackung als Prüfkriterium für die Echtheit genutzt. Im Beitrag werden verschiedene Varianten der Gewährleistung der Fälschungssicherheit bzw. des Nachweises von Fälschungen über aktuelle optische, magnetische und andere Verfahren vorgestellt und bewertet:

- Buchstaben-Zahlen-Kombinationen mit Validierung über IT;
- Hologramme;
- Mikro- und Nanopartikel;
- molekulare Markierungssysteme (DNA);
- Funk-Chips (RFID);
- Hardwareschutz (Dongle).

Allen gemeinsam ist die menschliche Intelligenz – welche den Fälschern allerdings ebenfalls nicht abzusprechen ist. Zu berücksichtigen ist aber, dass ein Fälscher 100% seiner Leistung zum Fälschen einsetzt, dagegen ein Produktentwickler höchsten 1% zur Fälschungssicherheit. Absolut nicht zu fälschen ist nur der Zufall! Im Beitrag wird deshalb auch ein auf Zufall basierendes Sicherheitssystem für Verpackungen vorgestellt.

Dietrich Balzer widmet sich dem Thema „Die gegenwärtige und zukünftige Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft“. Der Wirtschaftszweig „Sicherheit“ wird in der Wirtschaftsstatistik noch nicht ausgewiesen. National und international hat sich aber schon eine Sicherheitswirtschaft etabliert, wie wissenschaftliche Untersuchungen und Studien belegen. Auf Grund der spezifischen Eigenschaften der Automatisierungs- und Kommunikationstechnik spielt diese Technik in der

Sicherheitswirtschaft eine zentrale Rolle, die auf die Einheit von Informationsgewinnung, Informationsverarbeitung und Informationsnutzung zurückzuführen ist. Innerhalb der Sicherheitswirtschaft wird die Automatisierungs- und Kommunikationstechnik vor allem in folgenden Marktsegmenten eingesetzt:

- Sicherheitstechnik (Biometrie, Videotechnik, Sensorik, Leittechnik, Zutrittskontrolle);
- IT-Sicherheit (Netzsicherheit, Verschlüsselung, Virtual Private Network, Public Key Infrastructure, Smart Card);
- Sicherheitsdienstleistungen (Objekt- und Wachschutz, Risk Management, Trust Center, Sicherheits-Audits, Sicherheits-Engineering, Consulting).

Die Automatisierungs- und Kommunikationstechnik als sicherheitsorientierte Wissenschaftsdisziplin stellt für alle diese Marktsegmente Methoden und Produkte zur Verfügung, die auf die Kompensation nicht-ausregelbarer Störgrößen orientieren. Dabei geht er es vor allem um Lösungen der Prozessüberwachung sowie der vorbeugenden und elementaren Prozesssicherung. Die damit im Zusammenhang stehenden Probleme werden an Hand von Beispielen aus der Verfahrens- und der Fertigungsindustrie erläutert.

Die Darlegungen von *Mukayil Kilic* und *Klaus Fuchs-Kittowski* zu „Sicherheitsrisiken und Vermeidungsverhalten im Fall der modernisierten und neuen Informationsquellen bei der Lenkung und Remotefunktionen von Fahrzeugen“ auf dem Symposium können aus Datenschutz- und Geheimhaltungsgründen (leider) nicht abgedruckt werden. Es wurde deshalb nur die Zusammenfassung aufgenommen.

Gegenstand des Beitrages von *Annely Rothkegel* ist die „Sicherheitskommunikation“. Der Beitrag zielt auf unterschiedliche Konzepte des Schlüsselbegriffs Sicherheit, die in der Kommunikation über Technik und Technikgebrauch entwickelt und vermittelt werden. In fachlinguistischer Sicht sind es die Kontexte, die die sich stets verändernden Bedeutungen von Schlüsselbegriffen prägen. Dabei wirken Faktoren aus den jeweiligen Domänen und daraus abgeleiteten Szenarien sowie Merkmale der (Fach-)Gemeinschaften zusammen. Unterschieden werden Diskurs- und Praxisgemeinschaften. In Diskursgemeinschaften werden Sicherheitskonzepte entwickelt und diskutiert, u.a. im Sinne von Maßnahmen der Abwehr, des Schutzes oder der Resilienz. Praxisgemeinschaften sind dadurch gekennzeichnet, dass Alltagskontexte des Technikgebrauchs einbezogen sind. Damit erscheint der Horizont der Sicherheitsmodellierung weit ausgedehnt, die Kommunikation darüber aber eher eingeschränkt (z.B. Sicherheitshinweise in Produktinformationen, Wer-

bung). Neben klassifikatorischen Definitionen sind es vor allem implizite Modelle von Sicherheit (Situationen mit/ohne Gefahren), die die Kommunikation im Mix von Fach- und Alltagswissen prägen. Beide zusammen lassen sich wiederum in unterschiedliche Sicherheitskulturen einordnen. In einem übergeordneten Rahmen werden auf diese Weise technische Systeme mit gesellschaftlichen Systemen verbunden. Diskutiert werden die begrifflichen Grundlagen und linguistische Möglichkeiten der Analyse, die exemplarisch demonstriert werden.

Die Texte werden abgeschlossen mit Darlegungen von *Martin Endress* und *Benjamin Rampp* zu „Vertrauen in der Sicherheitsgesellschaft". Der Beitrag beschäftigt sich mit der Bedeutung unterschiedlicher Typen der Sicherheitsproduktion für verschiedene Modi des Vertrauens und dabei insbesondere den paradoxen Effekten der Herstellung von Sicherheit. Dazu wird, im Sinne eines Verständnisses gegenwärtiger gesellschaftlicher Konstellationen als „Sicherheitsgesellschaft", zunächst der Wandel des Sicherheitsverständnisses und in diesem Zusammenhang insbesondere das Phänomen des Risikos (und der Nebenfolgen) in spätmodernen Gesellschaftskonstellationen analysiert. Auf dieser Basis werden zwei Idealtypen der Sicherheitsproduktion und Regierung identifiziert und unterschieden: ein exkludierend-disziplinierender Typus sowie ein liberal-inkludierender Typus. Um deren Effekte auf Vertrauenskulturen zu analysieren, werden drei unterschiedliche Modi des Vertrauens differenziert: reflexives Vertrauen, habituelles Vertrauen und fungierendes (Grund-)Vertrauen. In Bezug auf diese Modi wird dann diskutiert, welche Verschränkungen von Vertrauensmodi und Typen der Sicherheitsproduktion bestehen, d.h. welche (Neben)Folgen die unterschiedlichen Typen der Sicherheitsherstellung jeweils für Vertrauenskonstellationen haben.

*****

Die Herausgeber bedanken sich bei all jenen, die sowohl zum Erfolg des 5. Symposiums zur Allgemeinen Technologie als auch zur Drucklegung dieses „Protokollbandes" beigetragen haben. Insbesondere zu nennen sind die Rosa-Luxemburg-Stiftung, die die Durchführung des Symposiums unterstützte, die Autoren, die den Forderungen der Herausgeber hinsichtlich Manuskriptgestaltung weitgehend nachkamen, und die Senatsverwaltung für Wirtschaft, Technologie und Forschung von Berlin, die die Drucklegung ermöglichte.

Literatur

Banse, G. (2009): Techniksicherheit und Sicherheitskulturen. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 195-215

Banse, G. (2011): „Normale Katastrophen“. In: Maring, M. (Hg.): Fallstudien zur Ethik in Wissenschaft, Wirtschaft, Technik und Gesellschaft. Karlsruhe, S. 160-166

Banse, G. (2013): Sicherheit. In: Grunwald, A. (Hg.): Handbuch Technikethik. Stuttgart/Weimar (im Druck)

Banse, G.; Reher, E.-O. (Hg.) (2002):Allgemeine Technologie – Vergangenheit, Gegenwart, Zukunft. Berlin (Sitzungsberichte der Leibniz-Sozietät, Bd. 50, H. 7)

Banse, G.; Reher, E.-O. (Hg.) (2004): Fortschritte bei der Herausbildung der Allgemeinen Technologie. Berlin (Sitzungsberichte der Leibniz-Sozietät, Bd. 75)

Banse, G.; Reher, E.-O. (Hg.) (2008): Allgemeine Technologie – verallgemeinertes Fachwissen und konkretisiertes Orientierungswissen zur Technologie. Berlin (Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 99)

Banse, G.; Reher, E.-O. (Hg.) (2011): Ambivalenzen von Technologien. Berlin (Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 112)

Banse, G.; Rothkegel, A.; Renn, O. (2009): Interdisziplinäre Sicherheits- und Risikoforschung. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 155-170

Belyová, L.; Banse, G. (2011): Safe Innovations, Innovative Safety. In: Loudín, J.; Hochgerner, J. (eds.): Social and Cultural Dimensions of Innovation in Knowledge Societies. Prague, pp. 67-80

Gronau, N.; Eversheim, W. (Hg.): Umgang mit Wissen im interkulturellen Vergleich. Beiträge aus Forschung und Unternehmenspraxis. München (acatech)

Hermeking, M. (2010): Technik und Kultur. Schnittstellen für die Interkulturelle Kommunikation. In: Banse, G.; Grunwald, A. (Hg.): Technik und Kultur. Bedingungs- und Beeinflussungsverhältnisse. Karlsruhe, S. 163-178

Meyna, A.; Peters, O. H. (1985/86): Handbuch der Sicherheitstechnik. 2 Bde. München/Wien

Perrow, Ch. (1987): Normale Katastrophen. Die unvermeidlichen Risiken der Großtechnik. Frankfurt am Main

Poy, A.; Weißbach, H.-J.; Florian, M. (1994): Arbeitssicherheit und Funktionssicherheit vernetzter Systeme. Opladen

Rösch, O. (Hg.) (2008): Technik und Kultur. Berlin

Schneider, J. (Hg.) (1991): Risiko und Sicherheit technischer Systeme. Auf der Suche nach neuen Ansätzen. Basel u.a.

Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.) (2009): Sicherheitsforschung – Chancen und Perspektiven. München (acatech)

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 21–31*

Lucia Belyová, Gerhard Banse

Sicherheit und Sicherheitskultur

1. Sicherheit und ihre Entwicklung

„Tag eins nach dem Meteoritenhagel im Ural: Die Bewohner von Tscheljabinsk räumen die Trümmer weg und sind heilfroh, dass die kosmische Attacke keine noch schlimmere Katastrophe verursacht hat“ (Spiegel 2013). Am 15.02.2013 wurden 1200 Menschen verletzt, als im russischen Tscheljabinsk ein Meteorit auf die Erde stürzte. Vor diesem Meteoritenregen wurde nicht gewarnt, seine Folgen und Auswirkungen ließen sich nicht vorhersehen und es ist ebenso nicht klar, welche Konsequenzen daraus für die Zukunft gezogen werden können. Was aber nach einem solchen Ereignis deutlich wurde, ist die Tatsache, dass es sich dabei um das Eintreten eines sehr unwahrscheinlichen Ereignisses, eines „schwarzen Schwans“, handelte. Ein schwarzer Schwan ist ein Ereignis, das unvorhersehbar und unberechenbar ist und gleichzeitig sehr weitreichende Auswirkungen hat (vgl. Taleb 2007). Ausgehend von der Definition des Risikos verbindet sich bei solchen Ereignissen eine verschwindend geringe Eintrittswahrscheinlichkeit mit einem großen Schadensausmaß. Diese Dualität führt, wie auch im Fall des Meteoritenhagels, oft dazu, dass gegen das Auftreten eines Schadensfalls fast keine Vorkehrungen getroffen werden können. Zusammenfassend kann man bei einer solchen Katastrophe weder die Folgen vorhersehen noch die Ursachen beheben.

Existenziell wichtig werden solche Ereignisse, wenn sie menschliche Sicherheitsbedürfnisse betreffen. Sicherheit gehört zu den grundlegenden Bedürfnissen des menschlichen Lebens. Der Maslowschen Pyramide zufolge stehen Sicherheit, Stabilität und Geborgenheit gleich an der zweiten Stelle hinter den physiologischen Bedürfnissen des Menschen wie Nahrungsaufnahme oder Schlaf (vgl. Maslow 1943).

Während sich der Meteoritenhagel nur wenig oder gar nicht von Menschen kontrollieren lässt, existiert jedoch ein weites Feld an Ereignissen, bei denen die Gewährleistung von Sicherheit durch Menschen maßgeblich beein-

flussbar ist. Dies gilt insbesondere für die Planung, Gestaltung, Umsetzung und Nutzung technischer Systeme. In einem sozio-technischen System kann ausschließlich der Mensch derjenige sein, der die Verantwortung für die Herstellung und Verwendung von Technik übernimmt, denn Verantwortung bedeutet (in sehr genereller Weise) „das Aufsichnehmen der Folgen des eigenen Tuns, zu dem der Mensch als sittliche Person sich innerlich genötigt fühlt, da er sie sich selbst, seinem eigenen freien Willensentschluß zurechnen muss" (Wörterbuch 1955; differenzierender vgl. z.B. EuS 1994).

Vor diesem Hintergrund verwundern die Ereignisse, die immer wieder bei der Entwicklung technischer Systeme entstehen. Letztes Beispiel dafür sind die Probleme des Boeing-Konzerns mit dem Großflugzeug 787 „Dreamliner". Dieses darf aufgrund eines Verbotes der US-Luftfahrtaufsicht FAA momentan nirgendwo auf der Welt starten. „Eine Boeing 787 musste im japanischen Takamatsu notlanden. In der Kabine hatte sich nach einem Batteriefehler Rauch entwickelt. [...] Es war der bisher letzte Vorfall in einer Reihe von Pannen an Bord der Dreamliner binnen weniger Tage" (SZ 2013a). Daraufhin wurde die Auslieferung weiterer Maschinen gestoppt. Die Ursachen für diese Pannen betrafen jeweils unterschiedliche Teile der Maschine: Risse der Cockpitscheiben, diverse Ölleckagen, Probleme mit den Bremsen und Batteriefehler, durch die Feuer verursacht wurden. Vor dem Hintergrund dieser verschiedenen und vielfältigen Probleme erscheint folgende Aussage von Boeing-Chef McNerney umso verwunderlicher: „Wir sind überzeugt, dass die 787 sicher ist" (SZ 2013b).

Die Vorfälle bei Boeing stehen bei weitem nicht singulär in der Liste sicherheitskritischer Ereignisse. Sie kann beispielsweise mit Triebwerksproblemen beim Airbus 380 oder mit der Deepwater Horizon-Katastrophe im Golf von Mexiko im Jahr 2010 fortgesetzt werden.

Wenn Sicherheit eine so wichtige Rolle in unserem Leben einnimmt, wieso ist ihre Vernachlässigung kein Einzelfall? Für die Beantwortung dieser Frage lassen sich mehrere Ursachen anführen. Sicherheit an sich gehört nicht zum produktiven Bereich der Wertschöpfung im Unternehmen, sondern bildet eine ihrer Voraussetzungen. Sicherheit zeigt sich daran, dass im Unternehmen „nichts passiert", also keine Material- und Personenschäden entstehen. Dies ist auch der Grund dafür, dass Sicherheit nicht immer präsent wird. Ihre Wichtigkeit wird oft erst dann sichtbar, wenn „es bereits zu spät ist", d.h. wenn der Schaden schon eingetreten ist. Erst dann werden sich in der Regel alle Beteiligten ihrer Bedeutung bewusst.

2. Gewährleistung von Sicherheit

Sicherheit stellt ein komplexes Phänomen dar, dessen Gewährleistung einen ständigen Prozess erfordert. Basierend auf den Definitionen nach Fahlbruch und Kaufmann bezeichnet Sicherheit das Funktionieren einer Entität ohne größere Zusammenbrüche oder Schäden für die Organisation und die Umwelt. Sicherheit ist ein dynamischer Prozess, der aus dem Zusammenwirken von intra- und extraorganisationalen Faktoren entsteht, die sowohl die Aspekte der äußeren als auch der inneren (Selbst-)Sicherheit beinhalten (vgl. dazu Banse 2013; Belyová 2013; Fahlbruch et al. 2008; Kaufmann 1970).

Dieser Definition zufolge ist Sicherheit nicht nur ein Zustand sondern eine Leistung, die kontinuierlich sowohl innerhalb (bspw. durch die Organisationsmitglieder) als auch außerhalb (bspw. durch gesetzliche Richtlinien und Regeln) eines Unternehmens erbracht werden muss. Für die Gewährleistung der Sicherheit ist die äußere Sicherheit (der Schutz vor Gefahren durch technische Sicherungsmaßnahmen) sowie die gleichzeitige Förderung der inneren Sicherheit (eines an einem sicherheitsorientiertem Handeln ausgerichteten Bewusstseinszustands oder des Besitzes von Fertigkeiten) von großer Bedeutung (vgl. dazu Kaufmann 1970). Wird nur ein Aspekt der Sicherheit betrachtet, beispielsweise indem nur die technischen Sicherheitsmöglichkeiten erhöht werden, so kann diese einseitige Betrachtung zu mehr innerer Unsicherheit führen. Dieses, auch „Ironie der Automatisierung“ genannte Paradoxon kann bei zunehmender Automatisierung die Verlagerung der Verantwortlichkeit in die Technik und gleichzeitig die Senkung der Handlungsfähigkeit des Akteurs verursachen (vgl. dazu Bainbridge 1987).

Den Grundhaltungen, Einstellungen und Kompetenzen der handelnden Personen, die die innere Sicherheit „ausmachen“, wird bei der Gewährleistung von Sicherheit eine entscheidende Rolle zugeschrieben. Diese „weichen“ Faktoren lassen sich nicht direkt quantifizieren, können aber insbesondere bei kritischen Situationen die Verhaltensweisen der Akteure stark beeinflussen. Eine auf solche Faktoren fokussierte Unternehmensstrategie zielt auf die Entwicklung einer adäquaten Sicherheitskultur, in der neben technischen und unmittelbar an den Benutzer adressierten Maßnahmen ebenso soziokulturelle Aspekte von entscheidender Bedeutung für die Sicherheit von bzw. in Technik-Mensch-Interaktionen sind.

3. Technik und Kultur

Der Kulturbegriff umfasst in einem breiten Verständnis folgende Bereiche des menschlichen Lebens und Handelns:

a. die Wertvorstellungen, Überzeugungen, Kognitionen und Normen, die von einer Gruppe von Menschen geteilt werden;
b. die Verhaltensweisen und Praktiken, die für eine Gruppe von Menschen üblich sind;
c. vergegenständlichte Artefakte, mit denen das Leben gestaltet wird;
d. „stillschweigend" vorausgesetzte Handlungs- und Verhaltens„regeln" (d.h. implizite „Werte").

Auch Technik lässt sich auf unterschiedlichen Ebenen abbilden (s. Tabelle 1).

Ebenen	**Interdependenzen zwischen Technik und Kultur zeigen sich in ...**
Materielle Ebene (betrifft den Umgang mit Technik als materielles Artefakt)	Technikgestaltung (Einfluss auf Prozess und Ergebnis); Umgang mit Technik (Nutzungsmuster) und/oder mit Infrastrukturen; verfügbaren Ressourcen
Kognitive Ebene (betrifft die Wissensordnungen, Bedeutungen und Nutzungsmuster im Umgang mit Technik)	Formen des und Umgang mit dem vorhandenen technischen Wissen(s) (etwa explizites und implizites Wissen); Zeichen, Symbolen und Wissenssystemen; Alltagswissen, „common sense"; Umgangstechniken (Wissen über den Umgang mit der Technik); Technologien (Wissensproduktion über Sachtechnik)
Normative Ebene (betrifft normative Vorstellungen in Bezug auf den Umgang mit Technik)	Bewertung des vorhandenen Wissens; der Deutungssysteme, Werte und Normen, Weltanschauungen, Selbstbilder, Vorannahmen
Ökonomische Ebene (betrifft wirtschaftliche Aspekte des Umgangs mit Technik, z. B. hinsichtlich Technikanschaffung, -wartung, -nutzung etc.)	Anschaffungs-, Betriebs-, Wartungs- und Instandhaltungskosten, Recyclingkosten etc. sowie Gebühren, die für technische Abnahmen entrichtet werden müssen

Tabelle 1: Ebenen der Beziehungen von Technik und Kultur
Quelle: Banse/Hauser 2010, S. 24

Kulturelle Einflüsse auf Technik beginnen mit der Entstehung von Technik und setzen sich mit ihrer Nutzung fort (vgl. näher dazu Banse 2010b; Banse/Hauser 2009). Dies gilt auch für sicherheitsrelevante Mensch-Technik-Interaktionen.

Die kulturelle Einbettung von Technik hat, bezüglich der Sicherheit, mindestens zwei Konsequenzen. Zum einen wird die Wahrnehmung von Gefahren, und damit auch der „Umgang" mit ihnen einschließlich des darauf basierenden „Sicherheitsverlangens", kulturell geprägt. Zum anderen bleibt die „Herstellung" von (technikbezogener) Sicherheit abhängig vom unterstellten Technik- und Techniksicherheits-Verständnis (vgl. auch Banse 2010a, 2011; Banse/Belyová 2013).

4. Sicherheitskultur

Die Auseinandersetzung mit Sicherheitskultur geht genauso wie der Begriff selbst auf die International Nuclear Safety Advisory Group (INSAG) zurück (vgl. INSAG 1988). Im Rahmen der Aufarbeitung der Reaktorkatastrophe von Tschernobyl betonte diese Kommission die Wichtigkeit kultureller Faktoren, vor allem in Form der Interaktion zwischen Mensch und Maschine. Dabei wurde klar, dass jede Gruppe von Personen bzw. jede Unternehmenseinheit einen eigenen Umgang mit Risiken entwickelt – eine eigene individuelle Sicherheitskultur (vgl. Müller et al. 1998). Die darauf zurückgehende, noch heute oft verwendete Definition von Sicherheitskultur lautet wie folgt: „Sicherheitskultur umfasst diejenigen Eigenschaften und Grundhaltungen in Organisationen und Personen, die dazu führen, dass Angelegenheiten, welche die nukleare Sicherheit der Anlage betreffen, mit vorrangiger Priorität ihrer Bedeutung entsprechend beachtet werden"[1] (vgl. INSAG 1991).

Sicherheitskultur besitzt dabei sowohl eine theoretische als auch eine praktische Ebene. Die theoretische Ebene wird charakterisiert durch Vorschriften, Anweisungen oder Regeln. Der Umgang damit, und zwar nicht nur im Sinne einer blinden Einhaltung, sondern auch ihrer Überzeugung und Akzeptanz, macht den Inhalt der praktischen Ebene der Sicherheitskultur aus. Bei der Operationalisierung von Sicherheitskultur auf die alltäglichen Prozesse und Aktivitäten eines Unternehmens wird aus dieser praktischen Ebene die Forderung nach einer gelebten Sicherheitskultur. Unter einer gelebten Sicher-

1 "Assembly of characteristics and attitudes in organisations and of individuals which establishes that, as an overriding priority, nuclear safety issues receive the attention warranted by their significance" (INASG 1991, p. 1).

heitskultur wird eine Sicherheitskultur verstanden, deren Notwendigkeit von allen Mitgliedern einer Organisation akzeptiert wird, an deren Gestaltung alle Mitglieder mitwirken und die permanent aufrechterhalten und verbessert wird (vgl. Belyová 2013).

Eine solche gelebte Sicherheitskultur erfordert Akzeptanz, Partizipation aller Beteiligten sowie kontinuierliche Verbesserung der einzelnen Bestandteile der Sicherheitskultur.

Akzeptanz betrifft hierbei sowohl Zweck als auch Mittel (vgl. Merton 1957). Dies setzt eine innere Überzeugung von der Sinnhaftigkeit der eingesetzten Maßnahmen voraus, um Sicherheit als gemeinsames Ziel im Fokus zu behalten. Dabei ist es wichtig, dass dieses Ziel von der Spitze eines Unternehmens festgelegt und vorgelebt wird, sich aber dennoch die Beteiligten aller Hierarchiestufen eines Unternehmens damit identifizieren können und an der Zielerreichung aktiv mitwirken (Partizipation). Da Sicherheitskultur nicht nur ein Zustand, sondern genauso einen Prozess darstellt, ist die Erreichung eines Idealzustandes nicht möglich. Dies liegt im Wesentlichen an sich ständig ändernden Rahmenbedingungen (beispielsweise neue Regelungen, neue Beteiligte). Deswegen stellt die kontinuierliche Verbesserung des jeweils erreichten Standes die dritte Voraussetzung einer gelebten Sicherheitskultur dar.

5. Operationalisierung

Da eine direkte Messung der Sicherheitskultur aufgrund der fehlenden harten Zahlen und Fakten nicht möglich ist (vgl. Hofinger 2008), kann sie nur anhand von Indikatoren vergleichbar beschrieben werden. Eine solche Operationalisierung stellt die „logische Verknüpfung zwischen dem nicht messbaren Tatbestand und dem zu messenden Indikator mittels einer Korrespondenzregel, die Angaben über die Art dieses Zusammenhangs macht“ dar (Stockmann 2007, S. 202). Kernprinzip der Operationalisierung ist die Definition eines Satzes von Indikatoren, der in seiner Summe das Konstrukt „Sicherheitskultur“ beschreibt. Die Indikatoren werden als Eigenschaften definiert, „die nicht direkt mit bestimmten Beobachtungen korrespondieren, sondern für deren Vorliegen bestimmte Beobachtungen lediglich als Indiz dienen können“ (Behnke/Behnke 2006, S. 29). Zur Entwicklung von Indikatoren sowie zur Operationalisierung der Sicherheitskultur existiert eine Reihe von Ansätzen und Modellen (vgl. dazu etwa Grote/Künzler 1996; Hudson 1999; Künzler 2002). Allerdings werden die dynamischen Aspekte der Sicherheitskultur, d.h. ihre Prozessbetrachtung, sowie Möglichkeiten der direkten Ableitung von Handlungsempfehlungen zur Verbesserung von

Sicherheitskultur anhand von konkreten Maßnahmen in den bestehenden Ansätzen nicht vollständig abgebildet (vgl. Belyová 2013).

Ein neuer Ansatz zur Operationalisierung von Sicherheitskultur betrachtet ein Unternehmen als ein sozio-technisches System und fokussiert demnach die unternehmensweite Erfassung von Sicherheitskultur, ohne auf die gesamtgesellschaftlichen sicherheitsrelevanten Zusammenhänge näher einzugehen (vgl. Belyová 2013). Das dort vorgestellte Modell zur Erfassung einer gelebten Sicherheitskultur besteht aus drei Teilbereichen (s. Abbildung 1):

- *Sicherheitsgrundstruktur,*
- *Sicherheitsakteure,*
- *Sicherheitsinhalte.*

Die *Sicherheitsgrundstruktur* besteht aus sechs Perspektiven, die prinzipiell eine Unternehmung ausmachen und einen Einfluss auf die Sicherheit haben können. Von einem sozio-technischen Systemansatz ausgehend, werden die Perspektiven Mensch, Technik und Organisation einbezogen. Um eine möglichst umfassende Liste an sicherheitskulturellen Einflussfaktoren zu erhalten, wird die Sicherheitsgrundstruktur um weitere drei Perspektiven – Dokumentation, Arbeitsbedingungen und Produkt – erweitert. Eine genaue Trennung zwischen einzelnen Perspektiven ist aufgrund der bestehenden Wechselbeziehungen nicht möglich und dient nicht dem Ziel der Unterteilung.

Bei der unternehmensweiten Erfassung von Sicherheitskultur ist die Frage nach der Auswahl von Unternehmensmitgliedern, die in die Befragung einbezogen werden, von großer Bedeutung. Auch wenn das Konstrukt der Sicherheitskultur die Summe der Eigenschaften und Grundhaltungen der Organisationsmitglieder darstellt, kann die Einbeziehung aller Mitglieder aufgrund des hohen Aufwands der Erfassung kaum gewährleistet werden. Aus diesem Grund werden die Vertreter einzelner Gruppen eines Unternehmens einbezogen, die eine Möglichkeit besitzen, die Sicherheit durch ihre Arbeitstätigkeit direkt zu beeinflussen. Die *Sicherheitsakteure* werden als Vertreter folgender Gruppen ausgewählt: Führungskräfte, Sicherheitsexperten (im Rahmen eines Unternehmens sind es meistens Fachkräfte für Arbeitssicherheit) und Mitarbeiter in der operativen Ebene eines Unternehmens.

Das verbindende Element zwischen Sicherheitsgrundstruktur und Sicherheitsakteuren bilden die *Sicherheitsinhalte*, also die sicherheitskulturellen Indikatoren, die in der Summe die Sicherheitskultur ausmachen. Diese orientieren sich an vier Phasen des kontinuierlichen Verbesserungsprozesses (KVP), einem qualitätswissenschaftlichen Ansatz der fortlaufenden Verbesserung (vgl. dazu Deming 1982). Die vier Phasen, auch PDCA-Zyklus ge-

nannt, bilden die Planung eines Prozesses (Plan), dessen Durchführung (Do), die Ergebniskontrolle (Check) und die Verbesserung oder Anpassung der Parameter (Act). Hinsichtlich der Erfassung der Sicherheitskultur bedeutet das, dass bei jedem Indikator ein SOLL-Zustand definiert und dessen Erfüllungsgrad ermittelt wurde, indem der IST-Zustand aus der subjektiven Sicht des Befragten abgefragt wurde. Je nach Differenzen zwischen dem Idealzustand und dem aktuellen Zustand des jeweiligen Indikators wurden weiterhin die Ursachen für die Unterschiede und die Verbesserungsmaßnahmen diskutiert.

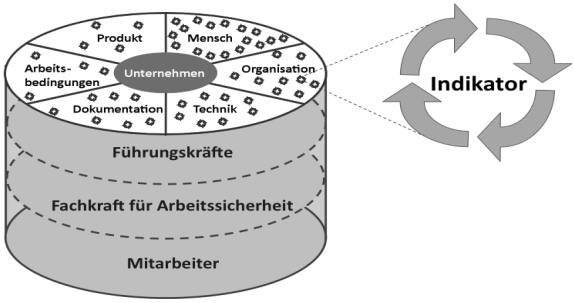


Abbildung 1: Erfassungsmodell einer gelebten Sicherheitskultur
Quelle: Belyová 2013

Für die Erfassung einer gelebten Sicherheitskultur anhand des beschriebenen Modells dienten als Grundlage zwölf Indikatoren. Diese wurden im Zuge einer Expertenbefragung (vgl. dazu Belyová 2013), an der Sicherheitsexperten aus Wissenschaft und Praxis teilgenommen haben, ausgewählt. Bei der weiteren Anwendung des Modells können zusätzliche Indikatoren hinzugefügt bzw. ersetzt werden, je nach Schwerpunkt oder Bedarf des jeweiligen Unternehmens. Die folgenden zwölf Indikatoren sind systematisch nach dem gleichen, an dem PDCA-Zyklus-orientierten Schema abgefragt worden:

1. Sicherheitsfokussierung
2. Verständlichkeit sicherheitsrelevanter Vorschriften
3. Kommunikation sicherheitsrelevanter Vorschriften
4. Dokumentation und Analyse sicherheitsrelevanter Vorfälle
5. Verhalten der Mitarbeiter in kritischen Situationen
6. Existenz von schriftlichen Vorgaben für den Umgang mit kritischen Situationen
7. Sicherheitsbewusstsein der Mitarbeiter

8. Strukturwissen der Mitarbeiter
9. Häufigkeit sicherheitsrelevanter Störungen an Maschinen und Anlagen
10. Risiko-, Gefährdungsbeurteilung und Belastungsanalysen
11. Prävention
12. Wertesystem im Unternehmen

Die Befragung wurde insgesamt in drei Unternehmen durchgeführt. Um eine Vergleichbarkeit der Unternehmen gewährleisten zu können, wurden produzierende Unternehmen ähnlicher Größe ausgewählt, die in der Maschinenbau-Industrie tätig sind und auf eine lange Tradition (von über 60 Jahren) zurückgreifen können. Aus jedem Unternehmen wurden drei Sicherheitsakteure entsprechend der drei Gruppen – Führungskräfte, Fachkräfte für Arbeitssicherheit und Mitarbeiter im operativen Bereich – interviewt.

Aus den einzelnen Interviews zu den Ausprägungen der zwölf ausgewählten Indikatoren lassen sich grob die folgenden Ergebnisse zusammenfassen (für eine detaillierte Auswertung vgl. Belyová 2013):

- Erst die Operationalisierung ermöglicht eine Vergleichbarkeit der Sicherheitskultur über mehrere Standorte und Unternehmen.
- Die Operationalisierung der Sicherheitskultur stellt meist schon den ersten Schritt zu ihrer Verbesserung dar, indem eine kritische Auseinandersetzung mit den einzelnen Indikatoren erfolgt.
- Sicherheitskultur in einem Unternehmen ist heterogen (bspw. auf unterschiedlichen Ebenen eines Unternehmens).
- Sicherheitskultur ist von einer Vielzahl von Faktoren abhängig; die einzelnen Indikatoren sollten eine hohe Ausprägung haben.
- Es existiert eine Vielzahl von Maßnahmen zur Erhöhung der Sicherheitskultur. Diese müssen aber umgesetzt und „gelebt“ werden.
- Unternehmen können auf dem Gebiet der Sicherheitskultur viel voneinander lernen.

6. Fazit

Vom Meteoritenhagel bis zur Entwicklung von Großflugzeugen – Sicherheit ist eines der Grundbedürfnisse des Menschen. Deshalb stellt die Erzielung sicherer Produkte und Prozesse eine elementare Aufgabe von uns allen und insbesondere von Unternehmen dar. Ein wesentlicher Stellhebel dafür ist die Erzeugung und Verbesserung der Sicherheitskultur. Diese lässt sich allerdings nicht ohne Weiteres messen und gezielt beeinflussen. Über eine systematische Methodik zur Indikatorenauswahl, -analyse und -optimierung wurde

ein Ansatz geschaffen, genau dieses Defizit aufzulösen. Anhand einer Anwendung in drei Beispielunternehmen zeigte sich die Praktikabilität des Ansatzes und es konnten Rückschlüsse auf Verbesserungspotenziale gezogen werden. Nichtsdestotrotz ist und bleibt Sicherheitskultur stark abhängig von Branchencharakteristika und den jeweiligen Umgebungsparametern. Aus diesem Grund bleibt es unumgänglich, mehr Erfahrungen in der Anwendung zu sammeln und die Validität der Systematik auch für weitere Bereiche zu ermitteln.

Literatur

Bainbridge, L. (1987): Ironies of Automation. In: Rasmussen, J.; Duncan, K.; Leplat, J. (eds.): New Technology and Human Error. Chichester a. o., pp. 271-283

Banse, G. (2010a): Techniksicherheit und Sicherheitskulturen. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 195-215

Banse, G. (2010b): Technisches und Kulturelles. Anmerkungen zu Interdependenzen. In: LIFIS ONLINE [08.03.2010]. – URL: http://www.leibniz-institut.de/archiv/banse_08_03_10.pdf [27.04.2013]

Banse, G. (2011): Im Fokus der Sicherheitsforschung: Sicherheitskulturen. In: Banse, G.; Krebs, I. (Hg.): Kulturelle Diversität und Neue Medien. Entwicklungen – Interdependenzen – Resonanzen. Berlin, S. 207-227

Banse, G. (2013): Sicherheit. In: Grunwald, A. (Hg.): Handbuch Technikethik. Stuttgart (im Druck)

Banse, G.; Belyová, L. (2013): Höhere Sicherheit durch bessere Sicherheitskultur?! In: Banse, G.; Hauser, R.; Machleidt, P.; Parodi, O. (Hg.): Von der Informations- zur Wissensgesellschaft. e-Society – e-Partizipation – e-Identität. Berlin, S. 415-427

Banse, G.; Hauser, R. (2009): Kultur und Technik: Genese und Stand einer Forschungsinitiative. In: Teorie vědy. Časopis pro teorii vědy, techniky a komunikace / Theory of science. Journal for theory of science, technology & communication, Vol. 31, No. 3-4, pp. 131-152

Banse, G.; Hauser, R. (2010): Technik und Kultur – ein Überblick. In: Banse, G.; Grunwald, A. (Hg.): Technik und Kultur. Bedingungs- und Beeinflussungsverhältnisse. Karlsruhe, S. 17-40

Behnke, J.; Behnke, N. (2006): Grundlagen der statistischen Datenanalyse. Eine Einführung für Politikwissenschaftler. Wiesbaden

Belyová, L. (2013): Kulturelle Faktoren qualitätsorientierter Unternehmensstrategien unter sicherheitsrelevanten Aspekten. Berlin

Deming, W. E. (1982): Out of Crisis. Cambridge, MA (Massachusetts Institute of Technology)

EuS (1994): Zweite Diskussionseinheit „Das Risiko im Prinzip Verantwortung“. In: EuS – Ethik und Sozialwissenschaften. Streitforum für Erwägungskultur, Jg. 5, H. 1, S. 109-194

Hofinger, G. (2008): Sicherheitskultur im Krankenhaus. Vortrag auf dem Rahmenkongress Medizintechnik und Patientensicherheit. Münster. – URL: http://www.gesine-hofinger.de/downloads/mek2008 sicherheitskulturimkrankenhaushofinger.pdf [01.02.2010]

Fahlbruch, B.; Schöbel, M.; Domeinski, J. (2008): Sicherheit. In: Badke-Schaub, P.; Hofinger, G.; Lauche, K. (Hg.): Human Factors. Psychologie sicheren Handelns in Risikobranchen. Berlin u.a., S. 19-33

Grote, G.; Künzler, C. (1996): Sicherheitskultur, Arbeitsorganisation und Technikeinsatz. Zürich

Hudson, P. (1999): Safety Culture – Theory and Practice. Paper presented at the RTO HFM Workshop on The Human Factor in System Reliability – Is Human Performance Predictable?, held in Siena, Italy, 1-2 Dezember, and published in RTO MP-032

INSAG – International Nuclear Safety Advisory Group (1988): Basic Safety Principles for Nuclear Power Plants. Wien (International Atomic Energy Agency)

INSAG – International Nuclear Safety Advisory Group (1991): Safety Culture. Safety Series No. 75-INSAG-4. Wien (International Atomic Energy Agency)

Kaufmann, F.-X. (1970): Sicherheit als soziologisches und sozialpolitisches Problem. 2. Aufl. Stuttgart

Künzler, C. (2002): Kompetenzförderliche Sicherheitskultur. Ganzheitliche Gestaltung risikoreicher Arbeitssysteme. Zürich

Maslow, A. H. (1943): A Theory of Human Motivation. In: Psychological Review, Vol. 50, pp. 370-396

Merton, R. K. (1957): Social Theory and Social Structure. London

Müller, S.; Brauner, Ch.; Grote, G.; Künzler, C. (1998): Sicherheitskultur. Spiegelbild des Risikobewusstseins. Zürich

Spiegel Online (2013): Tscheljabinsk nach Meteoritenhagel – Aufräumen in der Stadt der tausend Scherben. – URL: http://www.spiegel.de/wissenschaft/natur/tscheljabinsk-aufraeumen-nach-dem-meteoriten-hagel-a-883832.html [16.02.2013]

Stockmann, R. (Hg.) (2007): Handbuch zur Evaluation. Eine praktische Handlungsanleitung. Münster

Taleb, N. N. (2007): The Black Swan. London

SZ – Süddeutsche Zeitung (online) (2013a): Vom Dreamliner zum Albtraum-Flieger. – URL: http://www.sueddeutsche.de/wirtschaft/flugverbot-fuer-boeing-vomdreamliner-zum-albtraum-flieger-1.1575317[17.01.2013]

SZ – Süddeutsche Zeitung (online) (2013b): Boeing stoppt Auslieferung von Dreamliner. URL: http://www.sueddeutsche.de/wirtschaft/nach-pannenserie-boeingstoppt-auslieferung-von-dreamliner-1.1577367 [19.01.2013]

Wörterbuch (1955): Verantwortung. In: Hoffmeister, J. (Hg.): Wörterbuch der philosophischen Begriffe. 2. Aufl. Hamburg, S. 640

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 33–49*

Wolfgang Fratzscher

Über die Sicherheitskultur bei Kernkraftwerken

1. Bemerkungen zum Sicherheitsbegriff

Mit dem Sachverhalt Sicherheit ist ein Begriff ausgewählt worden, der in unterschiedlichen Bereichen ganz verschiedene Bedeutungen besitzt. Ihm geht es zunächst einmal so, wie es jedem Begriff ergeht, wenn er aus der Alltagssprache herausgenommen und in einer oder auch mehreren Disziplinen zum Fachbegriff wird. Die schärfere Definition in der Fachsprache bringt gegenüber dem Alltagsgebrauch eine Verminderung der Begriffsdeutung mit sich, wenn man so will, eine gewisse Verarmung.

Dabei bedeutet Sicherheit eine spezifische persönliche und gesellschaftliche Wert- und Bedürfnisvorstellung. So steht der Begriff Sicherheit zwischen der Gewissheit, die eine vollständige Sicherheit bedeutet, und dem Risiko, das Ausdruck der Unsicherheit mit dem möglichen Eintritt von Gefahren ist. Dabei sind diese Grenzen keinesfalls scharf. Vorstufen der Gewissheit können auf einer Meinung, auf einer Überzeugung oder auf Erfahrungen aus der Praxis, also auf Empirie, beruhen. So wird deutlich, dass die Gewissheit keine Eigenschaft des betreffenden Sachverhaltes ist, sondern eine psychische Position des Betrachters, des Subjektes, darstellt. Das Risiko ist die Möglichkeit eines Schadens, stellt mithin eine Gefahr, ein Wagnis dar.

So wird die Komplexität des Begriffes Sicherheit deutlich aus der Einordnung in die Begriffe Gewissheit und Risiko. Das lässt sich auch aus der historischen Entwicklung heraus belegen. Schlaglichtartig soll nur einmal die Position betrachtet werden, die im Jahre 1890 aus einem Konversationslexikon zu erkennen ist. Im „Meyer“ finden sich 11 Stichworte zum Begriff Sicherheit als zusammengesetzte Substantive, 6 davon betreffen technische Gegenstände, 3 finanzielle, 1 juristische und 1 militärische (vgl. Konversationslexikon 1890, S. 932-936). Die technischen Gegenstände sind der Sicherheitskessel, die Sicherheitslampe, der Sicherheitspfahl, die Sicherheitsröhre, das Sicherheitsventil und Sicherheitseinrichtungen wie Nottreppen, Alarmanlagen, Einrichtungen für Theater und Eisenbahnen für Notfälle, Rettungs-

boote und Schwimmwesten für Schiffe u.ä. Alles Dinge, die heute zur Sicherheitstechnik und zum Arbeitsschutz gezählt werden. Im Brockhaus aus den neunziger Jahren dagegen findet sich das Stichwort „Sicherheitstechnik" als Unfallverhütung und als Arbeitsschutz als einTeilgebiet der Sicherheitswissenschaft, die selbst nicht mehr als klassisches technisches Fach bezeichnet wird (vgl. Brockhaus 1993, S. 227-234). Es wird ausdrücklich vermerkt, dass zu dieser Disziplin neben der Technik die Sozial- und Geisteswissenschaften interdisziplinäre Aussagen beisteuern müssen. Dabei sind die Gegenstände der Sicherheitswissenschaften nicht nur der Unfall und der Schaden, sondern ausdrücklich auch das Risiko, dessen Limitierung, Reduzierung und Eliminierung.

2. Beiträge der Kerntechnik zur Entwicklung der Sicherheitskultur

Zu dieser enormen Entwicklung, die von der Funktionssicherheit technischer Anlagen über den Arbeitsschutz zu einer neuen und höheren Qualität der Sicherheitskultur geführt hat, hat die Kerntechnik einen wesentlichen Anteil beigetragen.

Die Voraussetzung dazu ist die konsequente Organisation der Sicherheitsmaßnahmen von kernenergetischen Anlagen zwischen Projektant und Betreiber einerseits und der Aufsichtsbehörde als Vertreter der Öffentlichkeit andererseits, wie vom Autor gezeigt worden ist (vgl. Fratzscher 2011, S. 131). Dabei spielt der Sicherheitsbericht, den der Projektant und Betreiber als Antragssteller anfertigen muss, eine zentrale Rolle. Er erschließt den vollständigen Sachverstand dieser Seite. Für die Genehmigung des Betriebes und damit der Sicherheit einer kerntechnischen Anlage ist in Deutschland die Gesellschaft für Reaktorsicherheit GRS gemeinsam mit der Reaktorsicherheitskommission RSK und dem Technischen Überwachungsverein TÜV verantwortlich. Die Wechselwirkung der Partner für atomrechtliche Genehmigungsverfahren zeigt Abbildung 1. In den sozialistischen Staaten war die strenge Teilung der Verantwortung zwischen Antragsteller und Genehmigungsbehörde unzureichend ausgebildet. In den kapitalistischen Staaten kann dieses System durch Lobbyarbeit und durch Korruption unterwandert werden. Seine ordnungsgemäße Funktion hat aber letztendlich dazu beigetragen, das heute erreichte Niveau der Sicherheitskultur mit den Erfolgen zu realisieren. Es kann betont werden, dass das dargelegte System im Wesentlichen auf den Einfluss von Ingenieuren zurückzuführen ist, die es aus den Erfahrungen mit dem Bau der ersten Kernkraftwerke heraus in den inhaltlichen Strukturen

abgeleitet haben. Darauf hat Joachim Radkau aufmerksam gemacht (vgl. Radkau 1994).

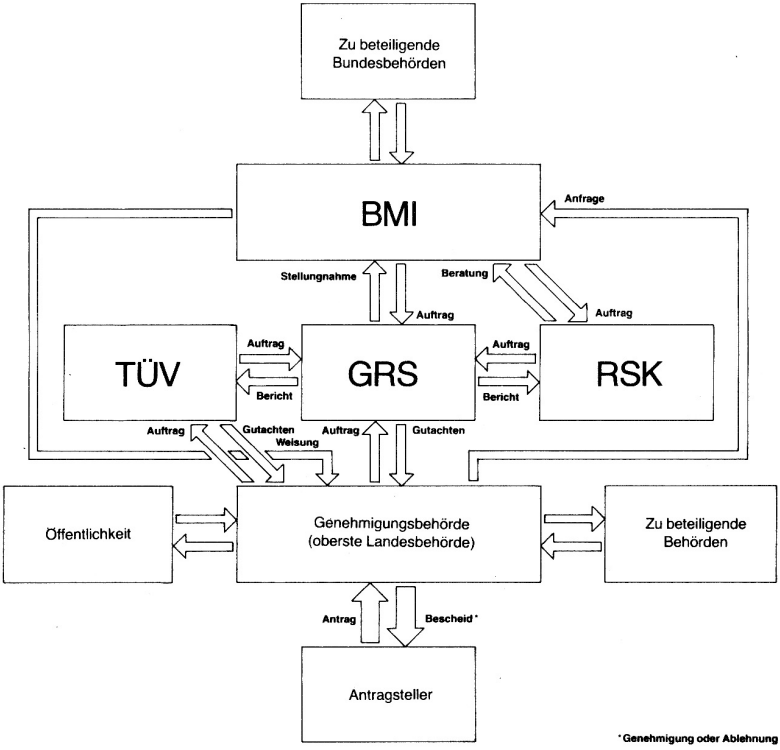


Abbildung 1: Aufsichtsbehörden
Quelle: Franzen/Wienhold 1989

Das ist auf folgende Sachverhalte zurückzuführen:

Die friedliche Nutzung der Kernenergie ist naturgesetzlich gebunden an das Auftreten von radioaktiver Strahlung. Der Mensch besitzt kein Sinnesorgan für die Erfassung dieser Strahlung. Die Atombombenabwürfe auf Hiroshima und Nagasaki zeigten der Menschheit nicht nur die ungeheure spezifische Energie von Kernreaktionen, sondern auch die massenhafte Einwirkung dieser Strahlung auf den menschlichen Körper. Die zentrale Aufgabe der Sicherheit kerntechnischer Anlagen ist deshalb der Schutz vor dieser Strahlung.

Bei der radioaktiven Strahlung kennt man die α- und β-Strahlung und die γ-Strahlung. Sie unterscheiden sich in ihrer Wirkung durch ihre Reichweite. Die Reichweite der α- und β-Strahlung ist relativ gering, die der γ-Strahlung sehr viel größer. Die Wirkung beider Strahlenarten ist aber vergleichbar. Den Schutzmaßnahmen müssen die unterschiedlichen Eigenschaften der Strahlenarten zugrunde liegen. So ist ein Schutz gegen γ-Strahlung primär durch Abstand halten zu erreichen, das beeinflusst z.B. die Standortwahl von Kernkraftwerken, oder durch entsprechende Abschirmungen. Die α- und β-Strahlung mit ihrer geringen Reichweite werden gefährlich, wenn sie durch Inhalation oder durch Inkorporation z.B. mit der Nahrung aufgenommen werden. Schutz gegen Isotope, die mit diesen Strahlenarten behaftet sind, ist deshalb nur möglich, wenn die Ursachen dieser Strahlenarten gegenüber der Umgebung durch gas- und druckdichte Barrieren oder Umschließungsbauwerke eingeschlossen werden. Für die Auslegung der Schutzmaßnahmen und für das Verhalten des Bedienungspersonals hat man für alle Strahlenarten Grenzwerte festgelegt, die sehr viel geringer sind als die Werte der natürlichen Strahlenbelastung, die jeder Mensch auf der Erde aufnimmt.

Als Schutzmaßnahmen gegen die radioaktiven Strahlen hat sich deshalb ein System von Barrieren in Kombination mit einem gas- und druckdichten Umschließungsbauwerk – dem Containment – als zweckmäßig erwiesen, wie es schematisch in Abbildung 2 dargestellt ist. Diese Bauweise soll auch eventuell auftretende Störfälle bis hin zu Katastrophen in dem Sinn beherrschen, dass die Umgebung des Kraftwerkes in diesen Fällen vor einer radioaktiven Belastung geschützt ist. Der Unfall in Three Mile Island hat bewiesen, dass ein solches System tatsächlich einen wirksamen Schutz gewährleistet, obwohl man damals noch nicht alle Unfallursachen, wie die gefürchtete Zirkon-Wasserstoff-Reaktion, kannte. Diese Maßnahmen machen deutlich, dass die Kerntechnik in der Sicherheitsphilosophie schon damit über den bei konventionellen Anlagen üblichen Auslegungsbedingungen hinausgegangen ist.

Das zeigt sich auch bei den Überlegungen zum Eindämmen der Auswirkungen, die auf menschliches Versagen zurückgeführt werden können. Bei der Auslegung der Schutzmaßnahmen wird als Leitgedanke eine fehlerverzeihende Technik angestrebt. Die Unfälle in Tschernobyl und Fukushima haben gezeigt, dass tatsächlich menschliches Fehlverhalten und unzureichend organisierte und undisziplinierte Eingriffe letztendlich zu diesen Katastrophen geführt haben. Deshalb ist diese Orientierung für die Sicherheitsphilosophie von essentieller Bedeutung. Auch das 30-Minuten-Konzept für die Gestaltung der Automatisierungsmaßnahmen für die Beherrschung von Störfällen dient der Eindämmung von möglichen menschlichen Fehlern, da damit

unmittelbare und möglicherweise unvollständig durchdachte Eingriffe der Bedienungsmannschaft vermieden werden sollen.

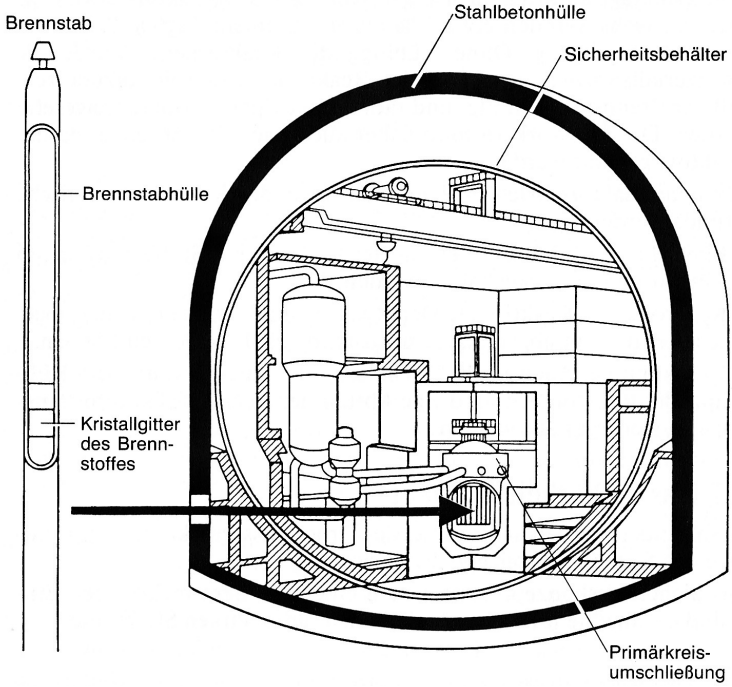


Abbildung 2: Aktivitätsbarrieren
Quelle: GRS 1989, S. 10

Ein weiterer Gesichtspunkt, der für die Gestaltung des Sicherheitssystems maßgebend ist, ist die Orientierung der Schutztechnik am Lebenszyklus der Anlage und nicht nur am Betrieb der kerntechnischen Anlagen. Das wird schon daran deutlich, dass im Sicherheitsbericht die Beschreibung der möglichen Störfälle der Anlage bis hin zum GAU (*G*rößter *A*nzunehmender *U*nfall) gefordert wird und dann die Ausarbeitung der erforderlichen technischen Systeme und organisatorischen Maßnahmen, die eine Beherrschung der Unfälle in einem Maße ermöglichen, die eine Belastung der Umgebung ausschließen soll.

Logischerweise hat auch die Stillegung kerntechnischer Anlagen einen Genehmigungsbedarf, ganz in Sinne der technologischen Sicherheit, die alle

Phasen des Reproduktionsprozesses umfassen sollte. Auch hierzu bedarf es eines spezifischen Sicherheitsberichtes, der alle Maßnahmen und mögliche Unfälle bis zur Herstellung des Zustandes der „grünen Wiese“ enthalten muss.

Ein weiterer Gesichtspunkt, der für die Ausprägung der Sicherheitsphilosophie für kerntechnische Anlagen wesentlich ist, ist nicht nur die Aufzählung und Angabe von Maßnahmen der Schutztechnik, sondern auch die Durchführung von Übungen unter Aufsicht der zuständigen Behörden. Da die möglichen Auswirkungen physikalisch bedingt sind und nicht z.B. durch juristische und nationale Grenzen zurückgehalten werden können, sind in der EU schon länderübergreifende Übungen dieser Art durchgeführt worden. So in Cattenom, einem französischen Kernkraftwerk, das nahe an der Grenze zu Deutschland und Luxemburg liegt. Es wird z.B. berichtet über eine Übung, die die Behörden von Frankreich, Luxemburg und Deutschland zur Zusammenarbeit in einem derartigen Fall zwangen (vgl. Chaton 2000).

In Verbindung mit dem Einfluss der Behörden ist aus der jüngsten Vergangenheit auf den Stresstest zu verweisen, der von der EU für die 145 in ihrem Verantwortungsbereich liegenden Kernkraftwerke in Folge des Unfalles von Fukushima angeordnet wurde.

Die angegebenen Sicherheitsaspekte führen bei ihrer Quantifizierung, die erforderlich ist, um die entsprechenden Schutzeinrichtungen auszulegen und Maßnahmen auszuarbeiten zur Eindämmung der Auswirkung von Störfällen, zu neuartigen theoretischen Problemen, die in der konventionellen Technik noch nicht in der Breite und Vollständigkeit gesehen worden sind. Das sind z.B. zur Quantifizierung von möglichen Unfällen benötigte Zuverlässigkeitsaussagen, die aus empirischen Angaben von Sicherheitsstatistiken oder aus theoretischen Überlegungen abgeleitet werden. Ihrem Wesen nach sind es Wahrscheinlichkeitszahlen, die in Grenzfällen die Werte Eins und Null annehmen können. Der Wert Eins gilt für das sichere Auftreten des Ereignisses, der Wert Null für den absolut sicheren Ausschluss. Für einen endlichen Zeithorizont ist der Wert Null nicht erreichbar, sodass ein gewisses sog. Restrisiko verbleibt. Für den Vergleich verschiedener technischer Schutzmaßnahmen untereinander ist die Verwendung derartiger Angaben sinnvoll.

Ein andere Gesichtspunkt, der sich aus dem vorgegebenen Rahmen ableiten lässt, ist der Sachverhalt, dass für die Auslegung von Sicherheitsmaßnahmen physikalische Grenzfälle zu postulieren sind, die die möglichen realen Belastungen umfassen, ohne dass z.B. die Anzahl der möglichen Übergangsprozesse, die in ihrer Vielzahl häufig gar nicht zu übersehen sind, im Einzel-

nen untersucht werden müssen. So hat man für die mechanische Belastung des Containments als Grenzfall den Abriss der Hauptumwälzleitung und den beidseitigen Ausfluss des Kühlmittelinhaltes angenommen. Ein weiteres Beispiel hierfür sind Annahmen, die gemacht werden müssen, um die Belastung von Druckräumen zu ermitteln, die über Zerreißbleche untereinander verbunden sind, um Kühlmittellecks aufnehmen zu können. Hierfür wurde z.B. die Annahme eines schlagartigen Druckausgleiches zugrunde gelegt. Eine solche Annahme unterdrückt zwar Effekte dynamischer Wirkungen, stellt aber für das Gesamtvolumen eine jeweilige maximale Belastung dar.

Verschiedentlich ist versucht worden, das Sicherheitskonzept der Kerntechnik auf andere Industriezweige zu übertragen. In den sechziger Jahren sind z.B. Überlegungen in der chemischen Industrie in dieser Richtung angestellt worden. Das ist auf heftigen Widerstand insbesondere aus den dort zuständigen Sicherheitskreisen gestoßen. Man befürchtete wohl die damit verbundenen wirtschaftlichen Belastungen. Obwohl die katastrophalen Unfälle z.B. von Soveso und Bophal gezeigt haben, dass genau in derartigen Dimensionen Sicherheitsüberlegungen angestellt werden müssten. Auch die jüngsten Unfälle mit Ölplattformen auf dem Meer zeigen, dass breiter angelegte Sicherheitskonzepte denkbar sind und damit Unfälle mit derartigen Zahlen von Unfallopfern und Umweltbelastungen vermeidbar erscheinen. Es scheint auch heute ein prinzipiell aufgeschlosseneres Klima in diesem Industriezweig vorhanden zu sein als vor 50 Jahren.

Aber auch neuere Untersuchungen haben gezeigt, dass im Bereich der chemischen Industrie derzeit noch nicht ein Entwicklungsstand erreicht ist, der Sicherheitsuntersuchungen mit allgemein vergleichbarem Niveau durchzuführen erlaubt. Damit Risikountersuchungen im Bereich der Chemie den Stand von Risikountersuchungen von Kernkraftwerken erreichen, wäre es u.a. erforderlich (vgl. Hauptmanns et al. 1987, S. 156)

- systematisch unter kontrollierten Bedingungen Zuverlässigkeitskenngrößen für Komponenten von Chemieanlagen zu erheben;
- Betriebserfahrungen systematisch auszuwerten, um einen zuverlässigen Überblick über mögliche störfallauslösende Ereignisse und deren Eintrittshäufigkeit zu erzielen;
- Modelle zur Beschreibung physikalischer und chemischer Phänomene wie Ausströmvorgänge (insbesondere bei Zweiphasen- und Mehrkomponentenströmungen) und Gaswolkenexplosionen zu entwickeln und experimentell abzusichern;
- Modelle für die Ausbreitung explosibler und toxischer Stoffe, insbesondere schwerer Gase unter Berücksichtigung der Erdoberflächenbeschaf-

fenheit und der Bebauungsstruktur in der Umgebung des Freisetzungsorts aufzustellen;
- Dosis-Risiko-Beziehungen für wichtige chemische Stoffe zu ermitteln.

Die Gesamtheit der Maßnahmen, die sich aus den Sicherheitsbemühungen insbesondere auch in der Kerntechnik ergaben, haben wohl auch einen wesentlichen Beitrag zur Herausbildung einer Disziplin Technologiefolgeabschätzung, kurz TA, geleistet. Man glaubte, durch eine systematische Durchdringung aller denkbaren Zustände einer beliebigen Technologie mit allen absehbaren Unfallfolgen ein methodisches Instrumentarium in die Hand zu bekommen, das die Genehmigungsinstitutionen der verschiedensten Art in die Lage versetzen, nicht nur eine technische Sicherheit, sondern auch einen Schutz der Umwelt und der Bevölkerung gewährleisten zu können. Damit sah man die TA als ein Mittel an, mit dem man in der Öffentlichkeit Aufklärung betreiben und Einsichten vermitteln konnte. Schon um 1994 gab es etwa 250 Bücher über diesen Gegenstand und wurden in der Forschung 110 Projekte gezählt (vgl. Conrady 1994). Deshalb gab man der TA eine besondere Rolle in der Politikberatung. So wurde in der Bundesrepublik beim Deutschen Bundestag ein entsprechendes Büro eingerichtet, das auch einen wesentlichen Einfluss auf einschlägige Einrichtungen in wissenschaftlichen Institutionen, wie den Hochschulen, nahm. Trotz erheblicher Anstrengungen und Bemühungen, die in dieser Richtung unternommen worden sind, sind wohl aus gesamtgesellschaftlicher Sicht die Erwartungen, die man von dieser Disziplin erhofft hatte, nicht erfüllt worden. Das führte dazu, dass einschlägige Institutionen in der Zwischenzeit schon wieder geschlossen worden sind.

Das liegt wohl letzten Endes daran, dass im Verlaufe der Entwicklung immer wieder nicht voraussehbare Zusammenhänge und Wechselwirkungen auftreten – die Zukunft ist eben offen –, die bei der systematischen Durchdringung der verschiedenen Technologien nicht berücksichtigt werden konnten. Andererseits kann in der Diskussion mit der Öffentlichkeit nur der Sachverhalt erschlossen werden, der rational darstellbar ist. Positionen, die auf Glaubens- oder Meinungsgrundlagen beruhen, sind nicht in die Richtung auf einen rationalen Kompromiss führbar. Man hat versucht, durch sog. Diskursverfahren unter Einschluss der Öffentlichkeit, aber unter Beteiligung von Fachleuten bestimmte offene Probleme bei größeren technischen Objekten einem Kompromiss zuzuführen. Dazu sind auch eine ganze Reihe von Veranstaltungen vorgesehen worden, die iterativ den Kompromiss erschließen sollten. Eines der bekanntesten Beispiele hierfür waren die Veranstaltungen,

die von Heiner Geißler in Verbindung mit dem Problem Stuttgart 21 durchgeführt worden sind. Das hat alles nicht den erhofften Erfolg gebracht.

Aus diesem Grunde hat man neben die objektive Rationalität, die durch entsprechende wissenschaftliche Durchdringung erschließbar ist, eine soziale Rationalität gestellt, die natürlich in gleicher Weise von der Politik wahrzunehmen ist. Sie äußert sich letzten Endes im Wählerverhalten.

Das führte schließlich dazu, dass von allen Bewertungskriterien, wie technische Funktionsfähigkeit, Wirtschaftlichkeit, Versorgungssicherheit, ästhetische Gesichtspunkte u.ä. bestenfalls die Nachhaltigkeit als Argument übrig bleibt. Dieser Begriff, der ja ursprünglich aus der Forstwirtschaft stammt, hat heutzutage auch sehr unscharfe Dimensionen angenommen, sodass damit unterschiedliche Entwicklungen gekennzeichnet werden können.

Das alles hat trotz aller Bemühungen in der Kerntechnik zu einem Misserfolg geführt – dem Ausstiegsbeschluss in Deutschland. Die gesamte Aufklärungskampagne hat trotz Hochglanzbroschüren und auch durch Unterstützung von den staatlichen Stellen keine positiven Ergebnisse gezeitigt.

So wird zumindest in der Kerntechnik eingeschätzt, dass in Zukunft für die Akzeptanz in Verbindung mit der Nachhaltigkeit die Sicherheit der technologischen Anlagen der einzige Maßstab sein wird. Früher wurden der Nutzen und die Wirtschaftlichkeit, natürlich unter Beachtung der Sicherheit, als Bewertungskriterien verwandt. Nach und nach rückte die Sicherheit an die erste Stelle, wobei die „Bezahlbarkeit“ zunächst noch eine bedeutende Rolle spielte. Heute ist offensichtlich die Sicherheit der alleinige Maßstab. Man muss bemerken, dass aus rationalen Gründen heraus diese Position nicht den Ausstieg bedeuten muss. Neuartige Leichtwasserreaktoren mit ertüchtigten Containmentsystemen und neuartige Reaktorkonzepte z.B. mit integriertem Brennstoffzyklus sind auch unter solchen Rahmenbedingungen denkbar. Auch die Entwicklungen von sog. „Kleinstreaktoren“ könnten mögliche Lösungen darstellen. Denn es wird bezweifelt, dass große Leistungen von Einzelanlagen, die im Wesentlichen aus ökonomischen Gründen angestrebt werden, unter dem Gesichtspunkt der Sicherheit noch vertretbar sind. Das setzt aber die Gültigkeit einer objektiven Rationalität voraus. Sind dagegen Glaubens- und Meinungspositionen in der öffentlichen Auseinandersetzung vorhanden, sind Lösungen in den angegebenen Richtungen nicht denkbar.

3. Technologische Strukturierung der Sicherheit

Die ungeheure Breite, die heute die Sicherheitswissenschaft angenommen hat, zwingt zur Systematisierung und auch Strukturierung. So sind im Angel-

sächsischen schon zwei Begriffe eingeführt worden – safety und security –, um einem solchen Ansinnen zumindest grob Rechnung tragen zu können. Dabei wird unter *safety* der Schutz der Umwelt vor Systemauswirkungen und unter *security* der Schutz des Systems vor Fremdeinwirkungen verstanden (vgl. Schnieder/Schnieder 2010). Ortwin Renn und Gerhard Banse haben den Begriff der Sicherheitskultur im deutschen Fachschrifttum publik gemacht, der 1986 in Folge der Reaktorkatastrophe von Tschernobyl geprägt worden ist (vgl. Banse 2010; Banse et al. 2010). Er soll eine Situation in der Gesellschaft beschreiben, wenn den Sicherheitsproblemen gesetzlich eine Priorität eingeräumt wird, die auch von Organisationen und dem Einzelnen getragen wird. Damit sind nicht nur die technischen, sondern auch die sozialen und kulturellen Aspekte Bestandteil des Begriffes Sicherheitskultur. Im Folgenden soll versucht werden, aus allgemeinen Überlegungen zur Technologie einen Vorschlag zur Systematisierung der Sicherheitsprobleme zu unterbreiten, der auch das jeweilige Niveau der Sicherheitskultur von Technologien verdeutlichen könnte und damit auch eine Einschätzung des Sicherheitsmanagements der verschiedenen Industriezweige und staatlichen Aufsichtsbehörden.

Unter Zugrundelegung der Annahme, dass die technologischen Systeme allgemein aus den Elementen Arbeitsmittel, Arbeitsgegenstand und Arbeitskraft zusammengesetzt sind, lässt sich der Begriff Sicherheit strukturieren und in weitere Dimensionen einordnen.

Beginnen wir bei den Arbeitsmitteln als der kennzeichnenden technischen Komponente. Auf der Ebene der Maschinen und Apparate als der materiellen Vergegenständlichung der Prozesseinheiten ist primär die Funktionssicherheit anzusiedeln (s. Abbildung 3). Sie soll eine permanente Verfügbarkeit des Arbeitsmittels gewährleisten, auch unter den Bedingungen einer unterschiedlichen Belastung. Man kann in diesem Zusammenhang auch von der Robustheit der technischen Gegenstände sprechen, die eine entsprechende Belastungsspanne z.B. durch Redundanzen oder auch „Sicherheitszuschläge“ zulassen. Im Allgemeinen wird in diesem Zusammenhang nicht unmittelbar von dem Begriff der Sicherheit als selbständigem Gegenstand gesprochen, sondern die hier einzuordnenden Überlegungen gehen als immanenter Bestandteil in die empirisch oder auch theoretisch begründeten Auslegungs- und Berechnungsgrundlagen der Maschinen und Apparate ein.

Die nächste Ebene betrifft das technische System, die Anlage als die materielle Hülle des Verfahrens. Hier kann man im Hinblick auf das Wechselspiel aller hierzu erforderlichen Elemente als von der Betriebs- oder auch Anlagensicherheit sprechen. Ihr zugrunde liegt die Einordnung und Anpas-

sung der Elemente. Es ist eine Art Systemsicherheit, die die Voraussetzung des möglichst störfreien Betriebes der Anlage über die gesamte Lebenszeit des technischen Systems ist. Dazu gehören dann auch Maßnahmen der planmäßigen vorbeugenden Instandhaltung, die in der Praxis häufig zugunsten anderer, insbesondere kurzfristiger ökonomischer Engpässe, vernachlässigt werden. Die Anpassung der Konstruktionswerkstoffe an die Anforderungen ist hierbei eine wesentliche Aufgabe. Das wird z.B. deutlich an den aktuellen Diskussionen über das Wechselspiel von Wärmedämmmaterial und Baustoff eines Gebäudes. Polymer und Beton oder Stein sind eben in vielfacher Hinsicht unterschiedlich.

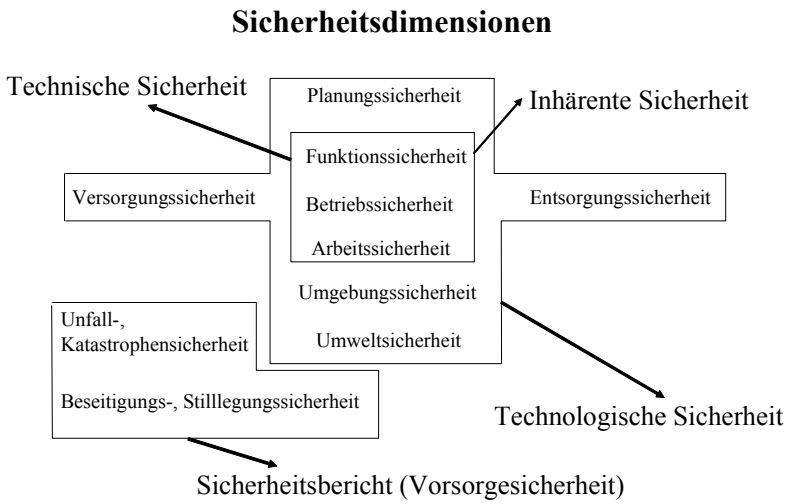


Abbildung 3: Technologische Struktur der Sicherheitsdimensionen
Eigene Darstellung

Neben dem Arbeitsmittel spielt für das erfolgreiche Arbeiten des technologischen Systems die Arbeitskraft eine wesentliche Rolle, unabhängig davon, in welcher Art und Weise die Arbeitskraft in das System eingebunden ist. Dieser Sachverhalt führt zu dem Begriff der Arbeitssicherheit oder auch des Arbeitsschutzes. Damit verbunden sind eigenständige technische Einrichtungen, die Aufgaben übernehmen, die über die Funktions- und Betriebssicherheit hinausgehen. Das führt – gegenüber vorherrschenden Betrachtungsweisen, bei denen üblicherweise die Sicherheitsüberlegungen immanenter Bestandteil der jeweiligen technischen Aufgabe waren – sowohl zu einem eigenständigen

Begriff der Sicherheitstechnik als auch zu einer mit der Entwicklung zunehmend eigenständiger werdenden technischen Disziplin Sicherheitstechnik. Ein Blick in Meyers Lexikon von 1890 lässt diese Situation schon erkennen. Insofern kann man die Einheit von Funktions-, Betriebs- und Arbeitssicherheit als das System der technischen Sicherheit bezeichnen. Insbesondere die Probleme, die mit der Entwicklung der Hochdrucktechnik auf dem Gebiet der Wärmetechnik verbunden waren, die im Havariefall zu den Dampfkesselexplosionen führten, lassen als nächstes Begriffsfeld das der Umgebungssicherheit erkennen. Bekanntlich war das der Ausgangspunkt für die Etablierung der Technischen Überwachungsvereine als selbständigen Institutionen in Gesellschaft und Wirtschaft. Damit war schon eine erste Stufe zur Herausbildung einer Sicherheitskultur zu erkennen. Auf der technischen Seite führte das zum Übergang von den Großwasserraumkesseln zu den Wasserrohrkesseln, die neben anderen Vorteilen insbesondere eine grundsätzliche Verminderung des Gefährdungspotenzials für die Umgebung darstellten. Dieser Ansatz wurde im Laufe der Zeit für viele weitere Belastungen der Umgebung übernommen, z.B. stofflicher oder akustischer Art. Auch wurden von dieser Seite Probleme aufgegriffen, die auf gesellschaftliche, vor allem soziale Wechselwirkungen zurückzuführen sind. Daraus entwickelte sich z.B. die Verkehrs- und die Bausicherheit.

Von der Umgebungssicherheit ist es nicht mehr weit bis zur Umweltsicherheit. Eine Position, die sich ursprünglich aus romantischen Einstellungen zur Natur entwickelt hatte, die aber heute weit darüber hinausführt. Sie führt bis hin zu Problemkreisen, die im angelsächsischen Sprachraum mit dem Begriff *security* bezeichnet werden. Im Gegensatz zu der Safety-Ebene, die etwa dem entspricht, was vorstehend mit dem Begriff der technischen Sicherheit, also der Sicherheitstechnik und dem Arbeitsschutz, gekennzeichnet worden ist. Sie führt also hin bis zu dem Schutz der technologischen Systeme vor willkürlichen bis hin zu terroristischen Ein- und Angriffen von außen. Ein Gefährdungspotenzial, das heute zunehmend in den Blick der Öffentlichkeit rückt.

Auf ein besonders makabres Beispiel wurde im Februar im Fernsehen hingewiesen. Militante Tierschützer hatten über Nacht aus einer Minkfarm, die zur Bereitstellung von Pelzen aufgebaut war, 20.000 Tiere freigelassen. Obwohl ein relativ großer Teil wieder eingefangen werden konnte, hat sich doch ein erheblicher Anteil in der Umgebung angesiedelt. Und das führte zu einer erheblichen Störung des biologischen Gleichgewichtes insbesondere in Vogelkolonien, da sich die Minke infolge des Fehlens natürlicher Feinde präch-

tig bis zu einer Plage entwickeln konnten und nahezu zur Ausrottung von ganzen Vogelarten führten.

Auch bei Großtechnologien wird dieser Gesichtspunkt im zunehmenden Maße diskutiert. Das sind die Dimensionen des Sicherheitsbegriffes, die sich für technologische Systeme aus dem Blickwinkel des Arbeitsmittels und der Arbeitskraft ableiten lassen.

Nun ist noch zu überlegen, welche Gesichtspunkte für die Sicherheitsdiskussion aus einer näheren Betrachtung des Arbeitgegenstandes folgen. Der Arbeitsgegenstand prägt zunächst den Charakter des technischen Systems. Es ist offensichtlich, dass die Sicherheitsprobleme unterschiedlich sind, je nach dem Zustand des Arbeitsgegenstandes und der Arbeitsweise des Systems. Der Zustand wird primär durch den Aggregatzustand bestimmt, für die Betriebsweise ist maßgebend, ob sie kontinuierlich, diskontinuierlich periodisch oder stochastisch ist. Für energetische Systeme ist maßgebend, ob z.B. Grundlast oder Spitzenlast gefahren werden soll. Die Zusammenhänge sind unmittelbar mit der jeweiligen Technologie verbunden und betreffen das Wechselspiel zwischen Arbeitsgegenstand und Arbeitsmittel. Das schlägt sich sicherheitstechnisch nieder in der Zertifizierung des Herstellungsprozesses, wie z.B. Schweißnahtüberprüfung und Dichtigkeitsprüfungen u.ä. Für allgemeine Überlegungen ist dann noch von Bedeutung, dass die Arbeitsgegenstände für den Betrieb der technologischen Systeme zur Verfügung gestellt werden müssen, wie auch die Erzeugnisse und Abprodukte oder Abfälle des Betriebes abgeführt und entsorgt werden müssen. Dazu ist einerseits die Versorgungssicherheit erforderlich und andererseits eine Absicherung für eine Entsorgungsmöglichkeit.

Wenden wir uns zunächst dem Problem der Versorgungssicherheit zu. Das betrifft unmittelbar die Sicherung der Zufuhr der erforderlichen Edukte, im speziellen der Rohstoffe oder Rohenergien für die technische Seite, aber auch die Zugriffsmöglichkeiten auf die notwendigen Arbeitskräfte. Die Zugriffsmöglichkeiten zu Energiequellen wie Kohle, Erdöl, Erdgas und Uran lassen auf der Energiestrecke die Probleme deutlich erkennen. Die mit den modernen Informationsmedien immer bedeutsamer werdenden seltenen Metalle oder Erden machen das Problem auf der Rohstoffseite in der aktuellen Diskussion deutlich. Aus der Arbeitskräftesituation erwachsen u.a. Standortprobleme und auch solche Probleme wie die Schaffung von Arbeitsmöglichkeiten für ausländische Arbeitskräfte usw. Sieht man von den notwendigen Aufbereitungstechnologien für Rohstoffe und von den Transporttechnologien für Energieträger und Rohstoffe ab, die jeweils selbständige technologische

Systeme darstellen, sind für die Versorgungssicherheit in erster Näherung ökonomische, soziale und politische Sachverhalte von Bedeutung. Das bedeutet, dass solche Gegenstände wie Versicherungen, Gesetze und Verträge der verschiedensten Art für die Herstellung der Versorgungssicherheit bedeutsam sind. Mit den jeweils zuständigen Institutionen entstehen so gleichfalls eigenständige Teildisziplinen in der Ökonomie, in der Justiz, in der Politik, die insgesamt Bestandteile der Sicherheitskultur sind.

Die Abgabe der Erzeugnisse, die Abführung der Abprodukte oder des Abfalls kann sich auch zu einem selbständigen Komplex entwickeln. Für die Abfuhr der Produkte ist die Marktsituation maßgebend. Die Abführung der Abprodukte oder des Abfalls des betrachteten technologischen Systems stellt in thermodynamischer Hinsicht den Hauptteil des Entropieexportes dar, der zu realisieren ist, um das im technologischen System angestrebte höhere Ordnungsniveau gegenüber der Umgebung zu erreichen. Stofflich gesehen steht in diesem Komplex nicht nur die Abfallwirtschaft mit den zugehörigen Deponien, sondern auch der Ansatz zum Stoffrecycling, der mit zunehmendem ökonomischem Wert der Rohstoffe immer größere Bedeutung erlangt. Energetisch fällt die Abfallenergie letzten Endes als Wärme an, was durch nachgeschaltete Systeme zur Kopplung oder auch zu regenerativen Aufgaben führen kann. Wenn man von den eigenständigen Systemen des Entsorgungskomplexes absieht, bedeutet die Entsorgungssicherheit für die betrachtete Technologie im Wesentlichen vertragliche Vereinbarungen, die rechtliche und ökonomische Beziehungen regeln sollen. Damit liegen die Probleme der Entsorgungssicherheit auf ähnlichen fachlichen Gebieten wie die der Versorgungssicherheit.

Das sind aber auch noch nicht alle Sicherheitsdimensionen, die aus technologischer Sicht zu verfolgen sind. Ordnet man das technologische System in den Reproduktionszyklus ein, so ist als eine wichtige Phase der Entwurf zu betrachten. Für diesen gilt neben der Einhaltung der aus den technischen Gegebenheiten folgenden Sicherheitsprinzipien die Planungssicherheit als eine wesentliche Voraussetzung für den positiven Abschluss der Arbeiten. Dahinter verbergen sich juristische – das Genehmigungsverfahren im weitesten Sinn – und vor allem finanzielle Sicherungen. Zur vollständigen Charakterisierung des Umfanges und des Niveaus der Sicherheitsproblematik gehört demnach auch dieser Komplex dazu.

Der Vollständigkeit halber muss in diesem Zusammenhang nun auch noch auf die endgültige Beseitigung der technologischen Systeme hingewiesen werden. Das beinhaltet, wenn es nicht dem Abfallkomplex zugeordnet

werden kann, den Abbau und die Demontage der betreffenden Anlagen bis zur „grünen Wiese“ als Endzustand. Das ist wieder ein eigenständiger technischer Komplex mit den zugehörigen Sicherheitsdimensionen und wird im starken Maße durch die Umweltsicherheit dominiert.

Das Zusammenspiel der aufgezählten Sicherheitskomplexe kennzeichnet das Niveau der Sicherheitskultur. Durch die Einbeziehung der vor- und nachgelagerten Systeme des betrachteten Objektes und seine Einordnung in den Reproduktionsprozess ist gegenüber der üblichen technischen Sicherheit zweifellos ein qualitativ höheres Niveau der Sicherheitskultur erreicht, das als die technologische Sicherheit bezeichnet werden kann.

Eine völlig neue Qualität der Sicherheitsüberlegungen wird erreicht, wenn neben den schon betrachteten technologischen Dimensionen auch noch die verschiedenen Zustände der technologischen Systeme einbezogen werden. Das bedeutet, dass neben dem Normalbetrieb, der bisher verfolgt wurde, auch die Havarie, der Unfall bis hin zur Katastrophe natürlich unter Einbeziehung der Auswirkungen auf die Umwelt in die Untersuchungen einbezogen werden.

4. Zur Situation

Es hat sich offensichtlich eine Schieflage in der Wahrnehmung der Sicherheit technischer Anlagen und der damit verbundenen Risiken in der Gesellschaft herausgebildet. Obwohl die Kerntechnik über das wohl vollkommenste System der Sicherheit ihrer Anlagen verfügt, wird sie von der Gesellschaft abgelehnt. Und das trotz der Tatsachen, dass z.B. bei dem Unfall von Three Mile Island das Sicherheitssystem funktioniert hat und keine Belastung der Umgebung entstanden ist. Auch bei dem katastrophalen Unfall von Fukushima, der in der INES-Bewertung mit der Stufe 7 eingeordnet werden muss, sind keine Strahlenopfer zu beklagen, weil mit Konsequenz eine entsprechende Evakuierung gefährdeter Gebiete vorgenommen wurde. Hier wie auch bei der Katastrophe von Tschernobyl war ursächlich menschliches Fehlverhalten Ausgangspunkt des Unfallgeschehens. Es ist schon darauf hingewiesen worden, dass in Tschernobyl und wahrscheinlich auch in Fukushima das ordnungsgemäße Wechselspiel zwischen Betreiber und Aufsichtsbehörde nicht möglich war oder nicht funktionierte.

Ragnar Löfstedt weist an anderen Beispielen auf die Schieflage der Bevölkerung in der Risikowahrnehmung hin (vgl. Löfstedt 2012). Er benutzt den Vergleich zwischen Dioxin verseuchten Eiern und dem Ehec-Virus. Obwohl nachweislich noch kein Bundesbürger durch Dioxin verseuchte Eier ge-

storben ist, wohingegen das Ehec-Virus schon zu einer Vielzahl von Todesfällen geführt hat, nehmen beide Entwicklungen einen vergleichbaren Stellenwert in der Wahrnehmung der Deutschen ein, wie entsprechende Untersuchungen gezeigt haben.

Er plädiert für eine risikobasierte Politik, die auf der Einführung eines dualen Konzeptes von Gefahr und Risiko beruht. Außerdem sollten Leitlinien für die Berichterstattung in den Medien als verantwortungsbewusste Vermittler ausgearbeitet werden unter verstärkter Einbeziehung von bestehenden Foren der Wissenschaftsmedien. Es geht also wieder, wie bei den Diskursverfahren, um eine frühzeitige Einbeziehung der Öffentlichkeit und nicht nur um die Untersuchung, sondern auch explizite Aufklärung. Ein schon absehbarer Effekt betrifft die Größe der technischen Anlagen. Aus ökonomischen Gründen sind die derzeitigen Größenordnungen realisiert worden. Diese Größe erfordert komplexe Sicherheitssysteme und -maßnahmen. Bei kleineren Anlagen kann häufig mit einem geringeren Umfang an Sicherheitstechnik und -organisation ein höheres Maß an Sicherheit und damit auch ein geringeres Risiko erreicht werden. Diese Konsequenz kann wohl für alle technischen Bereiche gezogen werden.

Aus rationalen Gründen bleibt noch übrig, auf die Schieflage in der Wahrnehmung der Gefahren und Risiken in der Gesellschaft zwischen Naturkatastrophen und technischen Anlagen hinzuweisen. Das hat sich deutlich bei dem Reaktorunfall von Fukushima gezeigt, lässt sich aber auch durch einen Vergleich von Unfallzahlen über einen langen Zeitraum nachweisen.

Literatur

Banse, G. (2010): Techniksicherheit und Sicherheitskulturen. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 195-215

Brockhaus (1993): Brockhaus Enzyklopädie in 24 Bänden. 19. Aufl. Bd. 20. Mannheim

Chaton, C. (2000): Atomarer Störfall als Planspiel. In: VDI-Nachrichten, Nr. 48. – URL: http://www.ingenieur.de/Fachbereiche/Kernenergie/Atomarer-Stoerfall-Planspiel [04.01.2013]

Conrady, H. (1994): Technikfolgenabschätzung in der Krise. In: VDI-Nachrichten (Archiv des Autors)

Franzen, L. F.; Wienhold, W. (1989): Sicherheit in der Kerntechnik. In: Arbeitssicherheit, Jg. 11, H. 3, S. 213

Fratzscher, W. (2011): Zu Risiken und Nebenwirkungen lesen Sie den Sicherheitsbericht oder fragen Sie ... In: Banse, G.; Reher, E.-O. (Hg.): Ambivalenzen von

Technologien – Chancen, Gefahren, Missbrauch. Berlin, S. 131-141 (Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 112)

GRS – Gesellschaft für Reaktorsicherheit (Hg.) (1989): Deutsche Risikostudie Kernkraftwerke, Phase B. Köln

Hauptmanns, U.; Herttrich, M.; Werner, W. (1987): Technische Risiken. Ermittlung und Beurteilung. Berlin u.a.

Konversationslexikon (1890): Meyers Konversationslexikon. Bd. 14. Leipzig

Löfstedt, R. (2012): EU-Regulierungsbehörden sollten sich nicht durch Schreckensnachrichten überrumpeln lassen. In: VDI-Nachrichten, Nr. 25 (Archiv des Autors)

Radkau, J. (1994): Angst und Angstabwehr als Regulative der Technikgeschichte. In: Kerner, M. (Hg.): Technik und Angst. Zur Zukunft der industriellen Zivilisation. Aachen, 53-72

Rothkegel, A.; Banse, G.; Renn, O. (2010): Interdisziplinäre Risiko- und Sicherheitsforschung. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 147-152

Schnieder, E.; Schnieder, L. (2010): Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 73-115

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 51–57*

Norbert Mertzsch

Sicherheitsaspekte beim Rückbau des KKW Rheinsberg

1. Vorbemerkungen

Das Thema „Sicherheit“ hat bei Stilllegung und Rückbau des Kernkraftwerkes Rheinsberg absolute Priorität. Oberstes Gebot aller Maßnahmen im Rahmen von Stilllegung, Demontage, Rückbau und Entsorgung der Kraftwerksanlage ist die Vermeidung von Gefährdungen für das Personal, die Bevölkerung und die Umgebung des Kernkraftwerkes.

Stilllegung und Rückbau des KKW Rheinsberg begannen mit Erteilung der Genehmigung Nr. I/95 zur Stilllegung und zum Teilabbau durch die zuständige Genehmigungsbehörde des Landes Brandenburg vom 28. April 1995. Im zugehörigen Genehmigungsverfahren nahmen Strahlenschutzbetrachtungen und Untersuchungen zu möglichen Auswirkungen der Rückbauarbeiten auf die Umwelt einen hervorragenden Platz ein.

Für den Abbau des Kernkraftwerkes Rheinsberg wurden insgesamt acht Abbauetappen vorgesehen. Dazu wurden jeweils eigene Genehmigungsanträge gestellt und nach umfangreichen Prüfungen entsprechende Genehmigungen erteilt. Dieser Weg wurde gewählt, um die Genehmigungsverfahren und die Realisierung der Abbauetappen übersichtlich zu gestalten. In den Genehmigungsanträgen und den untersetzenden Unterlagen für die Rückbauarbeiten werden die Ermittlung aller zu erwartenden Gefährdungen, nicht nur der radiologischen, sondern auch die anzuwendenden Rückbautechnologien, die vorzusehenden Sicherheitsmaßnahmen und die Entsorgung der Reststoffe und Abfälle beschrieben.

Alle Stilllegungs- und Rückbaumaßnahmen im KKW Rheinsberg werden durch Sachverständige, Strahlenschutzaufsichts- und atomrechtliche Genehmigungsbehörde begleitet.

Die Abbaureihenfolge beim Abbau der technologischen Anlage erfolgte von Bereichen geringer Dosisleistung zu Bereichen hoher Dosisleistung.

Parallel zur Stilllegung der Kraftwerksanlage läuft der Restbetrieb, innerhalb dessen Einrichtungen der Infrastruktur des Standortes weiterbetrieben werden, die für den Abbau der Anlage notwendig sind.

2. Strahlensicherheit

Strahlenschutzbetrachtungen besitzen bei allen Maßnahmen zur Stilllegung und zum Rückbau des Kernkraftwerkes Rheinsberg eine herausragende Bedeutung. Im Rahmen der Arbeitsplanung wurden und werden Maßnahmen zur Gewährleistung des Strahlenschutzes detailliert festgelegt. Maßgebend dafür ist die „Richtlinie für den Strahlenschutz des Personals bei Tätigkeiten der Instandhaltung, Änderung, Entsorgung und des Abbaus in kerntechnischen Anlagen und Einrichtungen Teil 2: Die Strahlenschutzmaßnahmen während des Betriebs und der Stilllegung einer Anlage oder Einrichtung“ (vgl. IWRS II).

Zu den Strahlenschutzmaßnahmen gehören zum Beispiel gerichtete Luftströmung im Arbeitsbereich und der Einsatz von Atemschutzmitteln, die sicherstellen, dass die Strahlenexposition des Rückbaupersonals durch freigesetzte Radionuklide (in Aerosolen) unterhalb der zulässigen Grenzwerte liegt.

Stark kontaminierte Bereiche werden mit einer Einhausung versehen, in der die Luft gesondert abgesaugt und gefiltert wird.

Der Einhaltung der zulässigen Grenzwerte der Direktstrahlung dienen Abschirmmaßnahmen in Bereichen hoher Dosisleistung. Dazu werden z.B. Bleimatten oder Abschirmwände eingesetzt.

Um die Strahlenschutzmaßnahmen festlegen zu können, erfolgt im Rahmen der Arbeitsplanung eine umfassende radiologische Aufklärung des zukünftigen Arbeitsbereiches. Dazu gehören Messungen der Dosisleistung und des Kontaminationszustandes an abzubauenden Anlagenteilen, im Arbeitsbereich und in angrenzenden Bereichen. Diese Messwerte dienen als Grundlage der Strahlenschutzplanung.

Abbaubegleitend erfolgen ebenfalls Messungen der Kontamination und der Dosisleistung, um die Einhaltung der Planwerte zu dokumentieren und um bei Abweichungen rechtzeitig reagieren zu können.

Um dieses leisten zu können, steht modernste Messtechnik zur Verfügung. Dazu zählen in den Abbaubereichen Aerosolsammler und -monitore sowie kontinuierlich anzeigende Dosisleistungsmessgeräte. Weiterhin werden Kontaminationsmessgeräte, Dosisleistungsmessgeräte mit Teledetektoren und Wischprobenahmetechnik mit zugehörigen Auswertegeräten

eingesetzt. Aerosolprobenfilter und Wischprobenfilter werden bei Bedarf nuklidspezifisch mittels Gamma-Spektrometrie ausgewertet.

Zur Auswertung und Bewertung der gewonnenen Ergebnisse wird erfahrenes Strahlenschutzpersonal eingesetzt (Strahlenwerker [VGB], Strahlenschutzfachkräfte [IHK], Strahlenschutzmeister und Strahlenschutzingenieure [VGB]).

Alle Messwerte werden dokumentiert und in umfangreichen Berichterstattungen, z.B. technischen Quartals- und Jahresberichten, bewertet.

Neben den radiologischen Messungen innerhalb der Kraftwerksanlage erfolgt die Umgebungsüberwachung des Kraftwerksstandortes auf Basis eines behördlich bestätigten Messprogrammes, abgeleitet von der Richtlinie zur Emissions- und Immissionsüberwachung von Kernkraftwerken (vgl. REI).

Die Abgabe von Radionukliden über die Abluft und das Abwasser während der Stilllegungsarbeiten wird durch technische Maßnahmen so begrenzt, dass die im Rahmen der Stilllegungsgenehmigung festgelegten Grenzwerte sicher unterschritten werden.

So werden alle Abluftströme vor der Abgabe aus Gebäuden oder Einhausungen über Schwebstofffilter der Klasse H 13 geleitet. Zum Nachweis der Einhaltung der Grenzwerte werden aus allen Abluftströmen Proben auf Filtern gesammelt (radioaktive Gase sind nicht mehr relevant) und gammaspektrometrisch auf kraftwerksspezifische Radionuklide sowie auf die Gesamtalpha-Aktivität untersucht.

Zusätzlich erfolgt an ausgewählten Standorten die Untersuchung von Bewuchs und Wässern auf Immissionen.

Wässer aus dem technologischen Teil der Kraftwerksanlage werden vor der Freigabe zur Abgabe homogenisiert, beprobt und auf kraftwerkstypische Nuklide analysiert. Zusätzlich werden alle den Standort verlassenden Wässer gammaspektrometrisch auf kraftwerksspezifische Radionuklide sowie auf die Gesamt-alpha-Aktivität untersucht. Die Ergebnisse dieser Messungen werden z.B. in den Umweltberichten der Energiewerke Nord GmbH dokumentiert. Überwachungsergebnisse der zuständigen Landesbehörde (LUGV) bestätigen diese Ergebnisse (vgl. LUGV 2012).

3. Physischer Schutz

Dem physischen Schutz von Kernbrennstoff wurde in der Nachbetriebsphase höchste Aufmerksamkeit gewidmet.

Um diesen entsprechend des geltenden Atomrechts der Bundesrepublik zu gewährleisten, erfolgten im KKW Rheinsberg zum bis dahin geltenden

Schutzniveau umfangreiche technische und organisatorische Nachrüstmaßnahmen. So erfolgte zum Beispiel der Zugang zu den technologischen Anlagen entsprechend der Zulassung des jeweiligen Mitarbeiters mit Hilfe eines kodierten Ausweises und eines Fingerprintsystems über Drehkreuze. Organisatorische Maßnahmen waren z.B. das Einsetzen von zuverlässigem Personal gemäß Atomrechtlicher Zuverlässigkeitsüberprüfungs-Verordnung (vgl. AtZüV 2010), das Siegeln von Behältern und Räumen mit Kernbrennstoff und umfangreiche abgestufte Kontrollgänge durch das Bewachungspersonal des KKW Rheinsberg in unterschiedlichen Kraftwerksbereichen. Zusätzlich gab es Beschränkungen im Publikumsverkehr.

Nach dem Abtransport des Kernbrennstoffs am 09. Mai 2001 in vier CASTOR-440/84-Behältern per Eisenbahn in das Zwischenlager Nord konnten die diesbezüglichen Sicherungsmaßnahmen deutlich reduziert werden, da sich das Gefährdungspotenzial im KKW Rheinsberg drastisch verringerte.

Für die weiteren Stilllegungs- und Rückbauarbeiten ist das Schutzziel „Rückhaltung radioaktiver Stoffe“ dominierend und wird sicher gewährleistet. Dazu dienen technische Maßnahmen, wie eine Fahrzeugschleuse zur Kontrolle aller das Kraftwerksgelände verlassenden Fahrzeuge.

Nichtradioaktive bzw. durch die zuständige Strahlenschutz-Behörde aus dem Geltungsbereich des Atomgesetzes entlassene Abfälle werden entsprechend Abfallrecht verwertet oder beseitigt. Zum Nachweis der ordnungsgemäßen Entsorgung werden für alle entsorgten Stoffe lückenlose Dokumentationen zu Herkunft, Materialart, Masse, Kontaminations- bzw. Aktivierungszustand und Entsorgungsweg geführt.

Darüber hinaus gibt es weitere organisatorische Maßnahmen, z.B. zu stichprobenartigen Personenkontrollen, Kontrollgänge durch das Bewachungspersonal usw.

4. Arbeitssicherheit

Ein weiterer wichtiger Sicherheitsaspekt beim Rückbau des KKW Rheinsberg ist die Arbeitssicherheit, denn Demontage- und Abbrucharbeiten gehören zu den Tätigkeiten mit dem höchsten Gefährdungspotenzial (vgl. Gabriel et. al. 2010). Das Gefährdungspotenzial besteht vor allem:

- in Gefahrstoffen (z.B. Asbest):
- im Umgang mit schweren Lasten:
- in der räumliche Enge;
- in möglichen statischen Problemen der Restanlagen und Gebäude.

Deshalb steht am Anfang der Planung der Rückbauarbeiten stets die Ermittlung aller zu erwartenden Gefährdungen (vgl. Rehtanz 1994). Verantwortlich für die Durchführung dieser Arbeiten ist der Bauherr, also das KKW Rheinsberg.

So sind alle Schadstoffe, die in der Anlage verbaut wurden, und nutzungsbedingt in der Anlage auftretenden Schadstoffe zu erfassen.

Zu den Schadstoffen in technischen und baulichen Anlagen des KKW Rheinsberg zählen:

- Asbest in schwachgebundener Form (Isoliermaterial oder Baustoffe wie Sokalit) und in festgebundener Form (Asbestzement),
- künstliche Mineralfasern – KMF (vorzugsweise als Isolierungen von Rohrleitungen und Behältern),
- polycyclische aromatische Kohlenwasserstoffe (PAK) in teerhaltigen Baustoffen wie Vergussmassen oder Dachpappen,
- Holzschutzmittel vorzugsweise in Dachbindern.

Zu den nutzungsbedingt in den technischen Anlagen und Gebäuden vorkommenden Schadstoffen zählen z.B. Verunreinigungen der Baustoffe durch Öle oder weitere im Gebäude verwendete Chemikalien, wie quecksilberbelastete Natronlauge und Salzsäure.

Auf Basis der erfassten Schadstoffbelastung werden die Rückbautechnologie (z.B. gesondertes Abstemmen von PAK belasteten Isolierungen) und die Entsorgungswege der entstehenden Abfälle festgelegt.

Beim Umgang mit schweren Lasten werden durch Sachkundige das Anbringen der Lastanschlagpunkte, der Einsatz von Kippvorrichtungen und Hebezeugen festgelegt. Erst nach Prüfung durch den Sachverständigen werden die Arbeiten freigegeben.

Die räumliche Enge in der Kraftwerksanlage, die sich unter anderem durch die Druckraumbauweise ergibt, erfordert erhöhte Aufmerksamkeit bei den Rückbauarbeiten.

Gegebenenfalls werden Zugänge für Rettungswege erweitert oder neu geschaffen bzw. es werden geeignete Rettungsmittel vorgehalten. Vor Demontagebeginn werden Rettungsübungen durchgeführt.

Weiterhin werden die Demontagewerkzeuge so ausgewählt, dass ihre Handhabung im Arbeitsbereich sicher möglich ist.

Beim Arbeiten in mehreren Ebenen wird sichergestellt, dass keine Gefährdungen durch herabstürzende Teile auftreten.

Beim Rückbau von Anlagenteilen wird die Rückbautechnologie so ausgelegt, dass eine statische Beeinflussung der restlichen Anlagenteile ausgeschlossen ist.

Beim Rückbau von Gebäudeteilen und dem Entkernen der Anlage, insbesondere dem Ausbohren oder Ausstemmen von Versatzteilen, Rissen und Löchern in Wänden, Böden und Decken sowie der Wandschwächung durch Abfräsen von Oberflächen, wird in Untersuchungen vorab geklärt, ob in allen Rückbauphasen die Statik des Restbaukörpers gewährleistet ist. Gegebenenfalls sind ausreichende Sicherungsmaßnahmen vorzusehen. Dazu erfolgen umfangreiche statische Berechnungen.

Auf der Basis dieser Erkenntnisse erfolgt die Planung der Vorgehensweise beim Rückbau. Diese wird dann beim Rückbau von Gebäuden in einer schriftlichen Abbruchanweisung festgehalten, in der für jeden Rückbauschritt die anzuwendende Technologie und alle notwendigen Sicherheitsmaßnahmen festgelegt sind (vgl. BGV C 22). So sind z.B. beim Ausbau von Rohrleitungen, die in der Wand verlegt sind, Schwerlastrüstungen einzusetzen.

Für die Bauleitung wird, wenn bei den durchzuführenden Arbeiten mehrere Firmen beteiligt sind, eine sachkundige Person als Koordinator eingesetzt.

5. Brandschutz

Große Bedeutung beim Rückbau des KKW Rheinsberg wird dem Brandschutz eingeräumt. Die Brandschutzmaßnahmen werden von der sicherheitstechnischen Regel der KTA 2101.1 „Brandschutz in Kernkraftwerken Teil 1: Grundsätze des Brandschutzes“ (vgl. KTA 2101.1) abgeleitet.

Zum einen befinden sich in der Kraftwerksanlage noch große Brandlasten (vorrangig Kabel), die erst im Laufe der Rückbauarbeiten verringert werden, und zum anderen würden durch einen Brand neben der Freisetzung chemischer Giftstoffe wie Salzsäure oder Dioxinen im Falle von PVC-ummantelten Kabeln auch radioaktive Aerosole freigesetzt.

Bei den festgelegten Maßnahmen handelt es sich im Sinne des vorbeugenden Brandschutzes um allgemeine Vorsorgemaßnahmen (zum Beispiel Hinweise zur Brandverhütung am Arbeitsplatz), im Sinne des abwehrenden Brandschutzes um Maßnahmen zur Rettung von Menschen und Maßnahmen zur Brandbekämpfung.

Im KKW Rheinsberg steht eine Betriebsfeuerwehr zur Verfügung. Vor Rückbau- und Demontagearbeiten werden in Abstimmung mit den Brandschutzbeauftragten die Brandschutzmaßnahmen (z.B. Einsatz mobiler Brand-

schutzwarnanlagen) angepasst und festgelegt. Dazu gehören auch technische Nachrüstmaßnahmen zur Verhinderung der Brandausbreitung, wie zum Beispiel der Einbau neuer Brandschutzklappen.

Literatur

AtZüV (2010): Verordnung für die Überprüfung der Zuverlässigkeit zum Schutz gegen Entwendung oder Freisetzung radioaktiver Stoffe nach dem Atomgesetz (Atomrechtliche Zuverlässigkeitsüberprüfungs-Verordnung – AtZüV) vom 1. Juli 1999 (BGBl. I, S. 1525), zuletzt geändert durch Artikel 1 der Verordnung vom 22. Juni 2010 (BGBl. I, S. 825). –
URL: http://www.gesetze-im-internet.de/atz_v/BJNR152500999.html [23.10.2012]

BGV C 22 (2010): Unfallverhütungsvorschrift Bauarbeiten BGV C 22 (VBG 37), gültig ab 1. April 1977 in der Fassung vom 1. Januar 1993 mit Durchführungsanweisungen vom Dezember 2010. –
URL: http://www.bgbau-medien.de/uvv/37/titel.htm [23.10.2012]

Gabriel, St.; Hofert, R.; Steinborn, V. (2010): Arbeitsschutz bei Abbrucharbeiten. 6. Aufl. Dortmund (hg. v. d. BAuA – Bundesanstalt für Arbeitsschutz und Arbeitsmedizin). –
URL: http://www.baua.de/de/Publikationen/Broschueren/A22.html [23.10.2012]

IWRS II (2005): Richtlinie für den Strahlenschutz des Personals bei Tätigkeiten der Instandhaltung, Änderung, Entsorgung und des Abbaus in kerntechnischen Anlagen und Einrichtungen Teil 2: Die Strahlenschutzmaßnahmen während des Betriebs und der Stilllegung einer Anlage oder Einrichtung (IWRS II) vom 17. Januar 2005. – URL: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_17012005_RSII3155061.htm [23.10.2012]

KTA 2101.1 (2000): Sicherheitstechnische Regel des KTA: KTA 2101.1 Brandschutz in Kernkraftwerken Teil 1: Grundsätze des Brandschutzes, Fassung 12/00. –
URL: www.kta-gs.de/d/regeln/2100/2101_1.pdf [23.10.2012]

LUGV (2012): Landesamt für Umwelt, Gesundheit und Verbraucherschutz – Brandenburg. – URL: http://www.mugv.brandenburg.de/cms/detail.php/5lbm1.c.163098.de [23.10.2012]

Rehtanz, H. (1994): Arbeits- und Umweltschutzanforderungen bei Rückbau, Demontage und Abriß von gefahrstoffbelasteten Industrieanlagen. In: Tepasse, R. (Hg.): Abbruch, Demontage und Rückbau von Industriestandorten und Großbauten Anforderungen an Arbeitsschutz und Umweltschutz. UTECH 1994 Umwelttechnologieforum Berlin, 24.-25. Februar. Berlin, S. 1-33

REI (2005): Richtlinie zur Emissions- und Immissionsüberwachung kerntechnischer Anlagen (REI) vom 07. Dezember 2005. – URL: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_07122005_RSII5156035.htm [23.10.2012]

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 59–78*

Dieter Seeliger

Fukushima – bisherige Lehren aus der Katastrophe über die Sicherheit von Kernkraftwerken

1. Ablauf der Havarie

Am 11.03.2011 um 14:46 Uhr Ortszeit ereignete sich etwa 150 km vor der Stadt Sendai ein Seebeben im Pazifik, welches mit der Magnitude 9,0 alle bis dahin in der Region bekannten (maximale Magnitude 8,2) übertraf. In seinem Wirkungsbereich lagen vier japanische Kernkraftwerke, darunter das KKW Fukushima Daiichi mit sechs Siedewasserreaktoren mit einer elektrischen Leistung von 4.547 MW, die in den Jahren 1971-1979 unter Nutzung US-amerikanischer Technologie von General Electric unmittelbar an der Meeresküste errichtet worden waren und vom japanischen Konzern TEPCO betrieben werden. Die Reaktoren sind mit einem primären Containment vom Typ MARK I ausgestattet: Das Reaktordruckgefäß aus Stahl befindet sich in einem „birnenförmigen“ Reaktorsicherheitsbehälter (Containment) aus Stahlbeton, der über Dampfleitungen an die ringförmig um den Reaktorsicherheitsbehälter angeordnete Kondensationskammer angekoppelt ist.

Das Beben hatte schwere Schäden an der Infrastruktur in der Region zur Folge, insbesondere den kompletten Ausfall des öffentlichen Stromnetzes und der Transportwege. Die für diesen Fall vorgesehene automatische Notabschaltung der in Betrieb befindlichen Reaktoren 1 bis 3 und die Einschaltung der Notstromversorgung mithilfe aller 13 hierfür vorgesehenen Dieselgeneratoren funktionierte reibungslos, ebenso wie die automatische Absperrung aller Durchführungen ins Containment sowie die Druckentlastung der Reaktordruckgefäße durch Ablassen von Dampf in die Kondensationskammern. Schäden an den Reaktoren traten bis dahin nicht auf bzw. wurden – zumindest zeitnah – nicht registriert, obgleich das Beben eine deutlich höhere Stärke aufwies als der Auslegung beim Bau des Kraftwerkes zugrunde gelegt worden war.

Ab 15:27 Uhr trafen nacheinander sieben Tsunamiwellen am Kraftwerksstandort ein, deren maximale Höhe mit 14 bis 15 Metern angegeben wird. Die

mit einer Höhe von 5,7 m ausgelegte Schutzmauer konnte die weiträumige Überflutung des Betriebsgeländes nicht verhindern, mehrere Gebäudekomplexe wurden im unteren Bereich überflutet, darunter die Keller der Maschinenhäuser, in denen sowohl die Notstromgeneratoren sowie teilweise auch die Batterien untergebracht waren. Es kam folglich sofort zum Ausfall der Notstromversorgung über Dieselgeneratoren für die Reaktoren 1 bis 4 und – dort, wo auch die Notbatterien von der Überflutung betroffen waren – zum schlagartigen kompletten Ausfall aller Kontroll- und Regulierungssysteme des Reaktors. Das bedeutete den Ausfall von Kühl- und Nebenkühlsystemen sowie der Frischwasserzufuhr für die Reaktoren und die zugehörigen Abklingbecken für benutzte Brennstäbe. Am gleichen Tag, um 15:42 Uhr, wurde der Notstand für Fukushima Daiichi ausgerufen.

Eine kurzzeitige Notkühlung von zwei Reaktoren ermöglichten noch betriebsbereite Batterien, danach gab es keine reguläre Kühlung der Reaktoren und der Abklingbecken. Es kam folglich sukzessive zur Überhitzung, Verdampfung des Wassers in den Reaktordruckgefäßen, teilweisem Freilegen der Reaktorkerne, Wasserstoffbildung durch katalytische Wasserzersetzung an den erhitzten Metallen der Reaktorkerne, starkem Druckanstieg. Durch automatisches Venting der Reaktordruckgefäße sollte deren komplette Zerstörung verhindert werden, dies war jedoch mit der Freisetzung an die Atmosphäre von Wasserstoffgas und flüchtigen Radionukliden, insbesondere J-131, Cs-134 und Cs-137, verbunden. Dies bedeutete eine starke radioaktive Belastung der Umwelt.

Am 12.03. um 12:57 Uhr zerstörte eine Wasserstoffexplosion die Reaktorhalle des Reaktors 1, einen Tag später folgte die Explosion am Reaktor 2, wobei die Hallenkonstruktion dabei weitgehend erhalten blieb. Am 15.03. wurde die Reaktorhalle 3 komplett zerstört, und am gleichen Tag kam es auch über dem nicht gekühlten Abklingbecken von Reaktor 4, in welchem 1331 Brennstäbe lagerten, ebenfalls zur Wasserstoffexplosion.

Ab 16.03. begann der Betreiber mit der Einleitung umfangreicher Notfallmaßnahmen: Evakuierungen aus der 20 km-Sperrzone, Kühlung der frei liegenden Brennelementbecken aus Hubschraubern mittels Wasserwerfern und Betonpumpen, schrittweise Wiederherstellung der Stromversorgung, Abdichtung von Lecks, Installation von Notkühlsystemen und weitere Maßnahmen. Eine ausführliche Analyse des Unfallablaufs ist im ENSI-Bericht (vgl. ENSI 2011) und anderen Quellen gegeben (vgl. ATF 2011; Kuczera 2011).

Um das fast unvorstellbare Maß der Auswirkungen dieses „größten anzunehmenden Nuklearunfalls“ auf die Bewohner der Region nachzuvollziehen,

muss man auch seine zeitliche Korrelation mit der Naturkatastrophe bedenken: Durch Erdbeben und Tsunami waren weite Küstenbereiche in der Region, viele Städte, Dörfer und Industrieanlagen verwüstet und über 20.000 Menschen waren verschollen oder umgekommen. Flüchtlinge und Obdachlose drängten in die umgebenden, höher liegenden Landstriche. In dieser Situation entwich aus dem KKW Fukushima Radioaktivität, vor allem in Form der flüchtigen Spaltprodukt-Nuklide J-131, Cs-134 und Cs-137, mit einer geschätzten Aktivität von etwa 10^5 Tera-Becquerel Jodäquivalent. Das entspricht einer Radioaktivität von 5 bis 10% der in Tschernobyl freigesetzten Menge. Aufgrund dieser Radioaktivitätsfreisetzung stufte die IAEA den Unfall in die höchste Stufe 7 der INES Skala (katastrophaler Unfall) ein (vgl. IAEA 2008). Eine Fläche von etwa 1500 km² wurde daraufhin zur Evakuierungszone erklärt und über 160.000 Bewohner wurden evakuiert! Vom Evakuierungsbefehl betroffen waren auch Gebiete, die Stunden oder Tage vorher von obdachlosen, traumatisierten Tsunami-Flüchtlingen aufgesucht worden waren! Nur ein glücklicher Umstand verhinderte noch gravierendere Auswirkungen auf die Bevölkerung Japans: Während infolge der Wasserstoffexplosionen kurzzeitig die höchsten Emissionsraten auftraten, herrschte am Standort Westwind, der die Radioaktivitätswolke nach Osten, in Richtung Pazifik trieb, der Großraum Tokio blieb daher weitgehend verschont. Später drehte der Wind und trieb eine bereits abgeschwächte „Radioaktivitätsfahne“ in Richtung Nord-West, in besiedelte Regionen, jedoch ohne Großstadt – auch Sendai blieb daher weitgehend verschont (vgl. GRS 2011). Die Freisetzung von Radioaktivität aus der Anlage in die Umgebung ist nachfolgend in den Monaten bis Februar 2012 sukzessive auf ein vergleichsweise sehr geringes Maß zurückgegangen (vgl. IAEA 2012).

2. Gegenwärtiger Stand und Perspektiven der Sanierung des Standortes

Nach einer gewissen Anlaufphase liefen – wie bereits erwähnt – zunächst umfangreiche Notfallmaßnahmen an mit dem vorrangigen Ziel, die Reaktorsicherheitsbehälter (Containment) und die Brennelementebecken durch äußere Kühlung vor Zerstörung durch Überhitzung zu bewahren. Hierfür kam – mangels Verfügbarkeit von Frischwasser – Seewasser zum Einsatz. Dies hatte die Ansammlung von großen Mengen (über 100.000 m^3) kontaminierten Salzwassers in den unteren Räumen der Reaktorgebäude zur Folge, welches ohne Reinigung und Dekontaminierung nicht ins Meer geleitet werden konn-

te – ein neues, gravierendes Problem. Infolge der Überflutung und der Wasserstoffexplosionen in den oberen Gebäudeteilen war das Kraftwerksgelände bedeckt mit Trümmerteilen, die als radioaktiver Abfall einer geordneten Zwischenlagerung zuzuführen waren. Die Außenwände der Anlagen und die Erdoberflächen im Kraftwerksgelände bedeckten radioaktive Nuklide, gebunden an Staubpartikel, Oberflächen oder Aerosole. Diese mussten durch Materialaustausch beseitigt oder mittels organischer Bindemittel (sog. Inhibitoren) fest eingebunden werden. Voraussetzung für alle Arbeiten waren die Verfügbarkeit von Elektroenergie und Frischwasser – neue Netzanbindungen mussten geschaffen werden. Die Liste sofort zu lösender Probleme und dementsprechender Sofortmaßnahmen war sehr groß.

Es folgten Maßnahmen, die für den Übergang zu einer kontrollierten Stilllegung der Anlage erforderlich waren. Hierzu zählt u.a. der Aufbau neuer Kreislauf-Kühlsysteme, welche eine kontrollierte Kühlung des Wassers in den teilweise gefluteten Sicherheitsbehältern und damit der Reste der zerstörten Reaktorkerne ermöglichen. Dazu mussten auch neue Wasserbehandlungsanlagen gebaut werden, mit denen das zirkulierende Kühlwasser und auch das akkumulierte Salzwasser aus den unteren Gebäudeteilen von radioaktiver Kontamination befreit werden kann. Die weitere Freisetzung und Ausbreitung von Radioaktivität über die Grenzen des Kraftwerksgeländes hinaus sollte schnellstmöglich verhindert oder zumindest weitgehend eingedämmt werden – Abdeckungen der teilweise freiliegenden Brennelementebecken, neue Einhausung der Reaktorgebäude, Abgasfilteranlagen, Spundwände bis in den Grundwasserbereich u.a. waren dafür notwendig und wurden bzw. werden gegenwärtig errichtet (vgl. IAEA 2011b, 2011c).

Alle genannten kurz- und mittelfristigen Maßnahmen waren schließlich einzubinden in einen Plan, welcher die langfristige Sanierung des Standortes, die Bergung des verbliebenen Brennstoffs sowie der hochradioaktiven Materialien (vor allem die Reste der Reaktorkerne und erstarrte uranhaltige Schmelze) und deren sichere Lagerung vorsieht. Der Betreiber arbeitete hierzu unter Kontrolle der japanischen Aufsichtsbehörden sowie im Kontakt mit internationalen Organisationen, insbesondere mit der IAEA, einen Masterplan unter dem Namen „Mid-and-long Term Roadmap“ aus (vgl. TEPCO 2012).

Die Sanierung verläuft seitdem planmäßig, mit hohem Tempo und transparent für die Öffentlichkeit. Hierzu werden von den japanischen Behörden regelmäßig sehr detaillierte Zustandsberichte und Datenanalysen veröffentlicht (vgl. JAIF 2011; JPG 2011). Die Internationale Atombehörde gibt zu-

sätzlich, basierend auf den japanischen Berichten und eigenen Expertenbesuchern vor Ort, regelmäßig „Fukushima Daiichi Status Reports“ heraus, in denen sehr ausführlich alle durchgeführten und demnächst vorgesehenen Teilprojekte sowie ausführliche Datenanalysen der Öffentlichkeit über das Internet frei zugänglich gemacht werden. Darüber hinaus sind weltweit auch zahlreiche einschlägige nationale Wissenschaftszentren und Aufsichtsbehörden mit der Auswertung, Analyse und Einschätzung des Unfalls befasst. In der Bundesrepublik Deutschland sind dies insbesondere das Karlsruher Institut für Technologie und die Gesellschaft für Reaktorsicherheit (vgl. GRS 2011). Die sichergestellte öffentliche Transparenz ist ein weiteres Merkmal, bei dem sich die Unfälle von Tschernobyl (in den ersten zehn Jahren nach 1986) und Fukushima unterscheiden.

Der heutige Zustand der Reaktoren in Fukushima soll anhand des Reaktors 1 dargestellt werden: Um das Reaktorgebäude wurde der Bau einer neuen Hülle aus einer Metallkonstruktion abgeschlossen, damit können alle Abgase und Dämpfe über Filtersysteme an die Atmosphäre abgelassen werden und radioaktiv belasteter Staub von Abrissarbeiten an Anlagenteilen verbleibt im Inneren. Der Innenbereich des Reaktorsicherheitsbehälters ist für eine direkte Messung vorerst weiterhin unzugänglich, so dass die Aussagen bisher auf Ergebnissen von Computermodellierungen basieren. Diese besagen, dass schlimmstenfalls ein (mehr oder weniger großer) Teil des Reaktorkerns geschmolzen, die Schmelze teilweise durch den Boden vom Reaktordruckgefäß hindurch getreten sein könnte und im 8 m starken Betonboden des Reaktorsicherheitsbehälters (Containment) aufgefangen wurde, ohne ihn zu durchdringen. Dort ist sie bereits beträchtlich abgekühlt und erstarrt. Auch in dieser Hinsicht unterscheidet sich Fukushima beträchtlich von Tschernobyl, wo infolge eines tagelangen offenen Reaktorbrandes (Graphit-Moderator!) durch die Kaminwirkung mit den Rauchgasen ein erheblicher Teil des langlebigen, hochradioaktiven Inventars in große Höhen der Atmosphäre transportiert wurde und ein anderer Teil der brennstoffhaltigen Lava in die Räume unter dem Reaktor geflossen sind.

Der Messung zugänglich sind dagegen Temperatur und Druck des Kühlwassers, welches über den neuen Kühlkreislauf von oben in das Reaktordruckgefäß eingeleitet wird, danach über die Reste des Reaktorkerns und die ggf. über die Schmelzrückstände am Boden des Reaktorsicherheitsbehälters läuft und in der ringförmigen Kondensationskammer gesammelt wird, von wo aus es in die Kühl- und Reinigungsanlagen zurückgeführt wird. In der Ta-

belle 1 sind Wasserfluss, Temperatur und Druck am Auslauf der Reaktoren R 1-3 aufgeführt (nach IAEA 2011a, 2011b, 2011c).

Reaktorzustand	**R 1**	**R 2**	**R 3**
Kühlwasserzufluss (m^3/h)	7,80	10,20	10,80
Druck im Containment (atm)	1,21	1,15	1,02
Ablauftemperatur (^oC)	43,80	71,40	70,70

Tabelle 1: Kühlzustand der Reaktoren R 1–3
Quelle: IAEA 2011a, 2011b, 2011c

Angestrebt wird als Nahziel die Erreichung des als „Kaltabschaltung" bezeichneten Zustandes der Reaktoren, der durch folgende Zielparameter gekennzeichnet ist: Ablauftemperatur des Kühlwassers < 100 ^{0}C; Druck am Auslauf 1 atm; minimale Radioaktivitätsfreisetzung, die an der Grenze des KKW-Geländes einer Dosisleistung < 1 mSv/a entspricht; Zirkulation und ständige Reinigung des Kühlwassers sowie Abdichtung aller Leckagen. Tabelle 1 belegt, dass hinsichtlich der Kühlung bis Anfang November 2012 bereits eine weitgehende Annäherung an diesen Zustand erreicht werden konnte.

Auch bei der Erkundung des radiologischen Zustandes im Inneren der Reaktorgebäude wurden Fortschritte berichtet. So enthält z.B. der IAEA Statusbericht vom 01.11.2012 Fotos und Messergebnisse für die Dosisleistung in den verschiedenen Ebenen des Reaktorgebäudes, die im Ergebnis von Ballon-Befahrungen in einem vertikalen Schacht der Gebäude ermittelt werden konnten. Die Messwerte liegen – abhängig von der Etage des Gebäudes – im Bereich von 20,1 mSv/h bis 150,5 mSv/h, was den ungeschützten Aufenthalt von Personal für Aufräum- bzw. Sanierungsarbeiten ausschließt. Bis zum endgültigen Abschluss der Sanierung der gesamten Anlage ist noch ein sehr langer und schwieriger Weg zu bewältigen: Die Bergung der Brennstoffreste aus den Reaktorsicherheitsbehältern 1-3 kann nur mit Hilfe von ferngesteuerten Robotern erfolgen. Die radioaktiv kontaminierten Abfälle sind zu verarbeiten und Vorsorge für die Endlagerung müssen getroffen werden. Die Kosten sind immens und derzeit noch nicht genau zu beziffern, die Zeitdauer bis zum Abschluss wird derzeit mit 40 Jahren angegeben (vgl. TEPCO 2012).

3. Zu den Ursachen des Unfalls

Die katastrophale Auswirkung der Tsunamiwellen ist in erster Linie auf eine mangelhafte Auslegung des Kernkraftwerkes gegen äußere Einwirkung bei seinem Bau in den siebziger Jahren zurückzuführen: Es war bekannt, dass in der Region Tsunamiwellen mit einer Höhe über 10 m statistisch einmal in 1.000 Jahren auftreten können. Selbst nach der einige Jahre vor dem Unfall erfolgten Erhöhung der Schutzmauer auf 5,70 m hätte sie häufiger zu erwartende kleinere Wellen nicht aufhalten können. Der Bau des KKW Fukushima, in einer von starken Erdbeben bedrohten Zone, hätte besser vermieden oder zumindest mit wesentlich stärkeren Sicherheitsvorkehrungen ausgerüstet erfolgen müssen.

Hinzu kommen technische Mängel bezüglich der Sicherheit, an erster Stelle eine unzureichende Redundanz und Diversität der Anlagen zur Nachwärmeabführung und zur Notstromversorgung. So war jeder Reaktor lediglich mit zwei Notstromdieselgeneratoren ausgestattet plus einem zusätzlichen Aggregat für die Gesamtanlage. Im Vergleich dazu sind KKW in Deutschland mit vier Notstromsystemen pro Anlage ausgestattet sowie neben der normalen noch mit einer Reservenetzanbindung, außerdem mit einer völlig unabhängigen Eigenbedarfsversorgung, der so genannten dritten Netzeinspeisung. In Fukushima waren weder Anlagen zur Rekombination von Wasserstoff noch Radioaktivitätsfilter in den Abluftanlagen installiert – nur so konnte es zu den zerstörenden Wasserstoffexplosionen und der Freisetzung großer Mengen flüchtiger Radionuklide von Jod und Cäsium kommen.

Auslegungsfehler beim Bau und damit unzureichender Schutz gegen Einwirkungen von außen betreffen außerdem auch folgende Aspekte: Die Notstromeinrichtungen lagen zu tief und waren nicht verbunkert, sondern in den Kellerräumen des Maschinenhauses quasi schutzlos der Überflutung auf dem KKW-Gelände ausgeliefert. Hinzu kam, dass ein Teil der Notstrombatterien ebenso tief und ungeschützt angeordnet war, wodurch diese sofort ausfielen, keine Kontroll- oder Steuerfunktionen mehr ausgeführt werden konnten und die Kontrollräume im Dunklen lagen. Das ist ein typischer Fall eines – bei sorgfältiger Planung tunlichst auszuschließenden – „Common-Cause Failure“, der in diesem Fall mehrere parallele Sicherheitssysteme gleichzeitig unwirksam machte.

Eine weitere Ursache liegt in offensichtlichen Mängeln beim Management begründet, vor und unmittelbar nach Eintreten des Unfalls. Genannt werden sollen hier: unzureichende technische und personelle Unfallvorsorge (zum Beispiel: sicher angelegte und ausreichende Lager von Ersatzteilen und

-komponenten), zögerliches oder gar verspätetes Handeln in den ersten Stunden und Tagen nach dem Unfall (zum Beispiel: spätes Einfliegen von Ersatzdieselgeneratoren). Vermutet werden muss auch, dass das nahe Ende der Laufzeit der Reaktoren das Management aus Kostengründen davon abgehalten hat, rechtzeitig noch Mittel in die Modernisierung der Sicherheitssysteme in Fukushima Daiichi zu investieren.

Die Analyse von Ablauf und Ursachen des Unfalls hält auch weiter an, so dass – obgleich die wesentlichen Zusammenhänge heute schon verstanden und publiziert sind – ein endgültiges Fazit noch zu ziehen sein wird. Eine Feststellung liegt heute schon auf der Hand: Es handelt sich bei der Katastrophe von Fukushima keinesfalls um das angebliche Eintreten eines Restrisikos, wie es vom Bundesverfassungsgericht 1978 mit der Umschreibung „unentrinnbare Ungewissheiten infolge der Grenzen menschlichen Erkenntnisvermögens“ definiert worden war. Zu den Unfallursachen werden in zahlreichen Publikationen Aussagen getroffen (vgl. AREVA 2011; ENSI 2011; GRS 2011 u.a.)

4. Radiologische Auswirkungen des Unfalls

Für eine vergleichende Bewertung betrachten wir zunächst die in Deutschland geltenden Jahresdosisgrenzwerte bzw. die mittlere Jahresdosis: Die mittlere Jahresdosis infolge natürlicher und zivilisatorischer Strahlungsexposition im Jahr 2008 betrug 3,9 mSv, davon sind 2,1 mSv auf natürliche Quellen und 1,8 mSv auf Röntgendiagnostik und Nuklearmedizin zurückzuführen. Der Jahresdosisgrenzwert für die Bevölkerung ist mit 1 mSv und der für strahlenexponierte Personen mit 20 mSv festgelegt. Der Gesetzgeber hat also zum Schutz der Bevölkerung für jeden Betreiber von Nuklearanlagen mit dem Jahresdosisgrenzwert von 1 mSv einen sehr geringen Wert angesetzt, deutlich unterhalb des Wertes, dem die Bevölkerung infolge natürlicher und zivilisatorischer Strahlungsexposition ohnehin ausgesetzt ist. Der Jahresdosisgrenzwert, der mit erhöhtem Krebsrisiko in Verbindung gebracht wird, beträgt 100 mSv, und ab 250 mSv werden erste klinisch fassbare Strahleneffekte beobachtet. Schwere Strahlenerkrankungen, die ohne Behandlung in 50% der Fälle zum Tod des Menschen führen können, treten ab 5000 mSv akuter Ganzkörperbestrahlung auf (vgl. GRS 2011).

Betrachten wir in diesem Licht die Strahlenexposition in Fukushima nach dem Unfall: In verschiedenen Medienberichten wurde besorgt über die Strahlenexpositionen des Kraftwerkspersonals und vor allem der Mitarbeiter von Fremdfirmen berichtet. Der Betreiber TEPCO registriert und publiziert regel-

mäßig die tatsächlich eingetretenen Strahlungsbelastungen und daraus abgeleitete Statistiken, die ebenfalls über IAEA-Statusberichte der Weltöffentlichkeit zugänglich gemacht werden. Tabelle 2 zeigt die statistische Auswertung der Strahlungsexposition für Eigen- und Fremdpersonal in dem entscheidenden Jahr 2011, geordnet nach Expositionsbereichen. Erfasst sind insgesamt 19.594 Personen, von denen in den beiden Expositionsbereichen bis 20 mSv bereits 16.209 Personen eingeordnet sind, das entspricht fast 82,7% aller Beschäftigten. Diese größte Gruppe befand sich also am Ende 2011 in einer Situation, die auch unter normalen Betriebsbedingungen einer Nuklearanlage in Deutschland zulässig gewesen wäre. Weitere 16,4% weisen Dosiswerte von 20 bis 100 mSv auf. Lediglich sechs Personen des Eigenpersonals waren einer Exposition über 250 mSv ausgesetzt, dies war ausschließlich im Zeitraum bis März 2011 der Fall. Es gibt bisher keine Todesfälle infolge zu hoher Strahlenexposition. An dieser Stelle sei auf die hohe Professionalität und umfangreichen Erfahrungen Japans – infolge der Atombombenabwürfe von Hiroshima und Nagasaki – auf den Gebieten Dosimetrie, Strahlenschutz und Umgang mit Strahlenerkrankungen hingewiesen.

Dosisbereich /mSv/	Gesamt	> 250	200 - 250	150 - 200	100 - 150	50 - 100	20 - 50	10 - 20	< 10
Eigen-personal	3.368	6	1	21	118	382	625	474	1.741
Fremd-personal	16.226	0	2	2	17	315	1.896	2.558	11.436

Tabelle 2: Strahlenexposition des Eigen- und Fremdpersonals in Fukushima im Jahr 2011
Quelle: IAEA 2012

Gravierende radiologische Auswirkungen betreffen Gebiete, welche durch Niederschläge von Cs-137 und Cs-134 belastet sind. Dies ist vorwiegend in nordwestlicher Richtung von Fukushima Daiichi der Fall, in einer relativ begrenzten Niederschlagsspur, die bis etwa 30 km vom Standort aus reicht. In diesem Gebiet liegen die Jahresdosiswerte bis 20 mSv, örtlich auch höher. Die meisten übrigen Gebiete weisen demgegenüber wesentlich geringere Belastungen aus, meist unter 5 mSv. Teilweise konnten nach Dekontamination von Oberflächen und Böden ursprünglich gesperrte Flächen bereits wieder freigegeben werden. Infolge der relativ langen Lebensdauer von Cs-137 ($T_{½}$ = 30,17 a) muss man davon ausgehen, dass die stark belasteten Landstriche noch für lange Zeit für die normale Besiedlung gesperrt bleiben werden.

Mit großer Sorgfalt erfolgen systematische Lebensmittelkontrollen in großen Teilen Japans. So wurden allein im Zeitraum vom 24.09.2012 bis 25.10.2012 in 45 Präfekturen 27.915 Proben von verschiedenen Produkten entnommen, von denen 27.707 ohne Befund waren bzw. unter den zulässigen Grenzwerten lagen. In Tabelle 3 wird ein (kleiner) Auszug für fünf Präfekturen wiedergegeben. Beispiele für belastete Proben in der Präfektur Fukushima betrafen u.a. Pilze (55 Proben), Schaffleisch (19 Proben) und Fisch (16 Proben).

Region (einige Beispiele)	**Proben gesamt**	**Proben belastet**
Fukushima	3.686	126
Tokyo	78	-
Iwate	2.309	14
Ibaraki	2.666	5
Miyagi	4.531	13

Tabelle 3: Einige Ergebnisse radiologischer Untersuchungen von Lebensmitteln
Quelle: IAEA 2012

Das Ministerium für Landwirtschaft hat daraus spezifische Empfehlungen für bestimmte Produkte und Regionen abgeleitet, so dass der Ausschluss des Verzehrs belasteter Produkte sichergestellt ist. In Anbetracht der ohnehin sehr geringen zulässigen Grenzwerte für die Belastung in Lebensmitteln kann man davon ausgehen, dass kaum reale gesundheitliche Gefährdungen eingetreten sind. Aber es bleiben noch für lange Zeit Angst und Verunsicherung bei der Bevölkerung vor der unsichtbaren Gefahr. Neben dem Verlust der Heimat infolge der Evakuierung ist dies wahrscheinlich die stärkste negative Auswirkung, die die Radioaktivitätsfreisetzung durch den Reaktorunfall von Fukushima für die Bewohner Japans hat.

5. Aktivitäten der IAEA nach dem Unfall

Die Internationale Atomenergieorganisation der UNO (IAEA) hat sofort nach dem Unfall umfangreiche Aktivitäten mit der Zielstellung aufgenommen, alle bekannt werdenden Fakten über Ursachen, Ablauf und Maßnahmen der japanischen Behörden zu dokumentieren und sie einer breiten internationalen Öffentlichkeit zugänglich zu machen. Hierzu werden regelmäßig Statusberichte publiziert, die im vorliegenden Beitrag bereits mehrfach zitiert wurden. Durch Expertenmissionen der IAEA vor Ort wird das Geschehen sachkundig

begleitet (vgl. IAEA 2011c). Das Hauptanliegen besteht darin, den Prozess der aktiven Umsetzung von Erkenntnissen über die Unfallursachen und daraus zu ziehende Lehren für die weltweite Verstärkung der Nuklearsicherheit in den Weltregionen sowie einschlägigen internationalen und nationalen Gremien der Mitgliedsländer zu stimulieren, zu fördern, öffentlich zu machen und in den einschlägigen internationalen Konventionen und Vorschriften über Nuklearsicherheit verbindlich festzuschreiben. Auch wenn die IAEA selbst nicht über Weisungsbefugnis gegenüber den Betreibern oder nationalen Aufsichtsbehörden verfügt, so kommt ihr doch, quasi als „nukleares Weltgewissen", eine überaus wichtige Rolle zu: Sie setzt die Maßstäbe für eine weltweit sichere Nutzung der Kernenergie, die von den Mitgliedsländern auf freiwilliger Basis in der Praxis implementiert werden. Außerhalb dieser Regeln zu agieren, ist für loyale Mitglieder der Weltgemeinschaft de facto ausgeschlossen, führt in die politische und fachliche Isolation.

Wenige Monate nach dem Unfall regte eine Ministerkonferenz die Aufstellung eines Aktionsplanes zur Stärkung der Nuklearsicherheit im Lichte der Ereignisse in Fukushima an, der von der Generalkonferenz der IAEA am 22.09.2011 abschließend verabschiedet wurde. Er sieht 12 Punkte zur Stärkung der Nuklearsicherheit vor, die sich – stark verkürzt – wie folgt zusammenfassen lassen (vgl. IAEA 2011a):

- umgehende Durchführung von Stresstests an allen KKW der Mitgliedsländer;
- Überarbeitung der geltenden IAEA-Vorschriften und Prozeduren zur Sicherheitsanalyse;
- Verstärkung der Einsatzbereitschaft und Reaktionsfähigkeit in Havariesituationen;
- Überprüfung der nationalen Sicherheitsbehörden und Erhöhung von deren Einsatzbereitschaft;
- Verbesserung der Managementsysteme und Sicherheitskultur der Betreiber;
- Überarbeitung der IAEA-Sicherheitsstandards;
- Implementierung aller existierenden internationalen Konventionen zur Nuklearsicherheit und gegenseitige Unterstützung in Notfallsituationen;
- fachliche Unterstützung von Staaten, die eigene nationale Nuklearprogramme beginnen;
- Ausbau der nationalen Kapazitäten für nachhaltige und sichere Nutzung der Nukleartechnik;
- Ausbau des Strahlenschutzes für Menschen und Umwelt mit den Aspek-

ten: Überwachung, Dekontaminierung, Sanierung inklusive Aus- und Weiterbildung dafür;
- Erhöhung der Transparenz, Effektivität und Kommunikation zwischen Operatoren, Regulatoren und den einschlägigen internationalen Organisationen;
- effektiver Einsatz von Forschung und Entwicklung für Nuklearsicherheit und -technologie.

Viele konkrete Schritte wurden bereits von diesem Aktionsplan in den Regionen angeregt oder in Gang gesetzt, darunter auch in der Europäischen Union. Die IAEA selbst organisiert u.a. zahlreiche internationale Konferenzen und Expertentreffen zu Einzelaspekten des Aktionsplanes, die dem Ziel dienen, die notwendigen Schritte zur Erhöhung der Nuklearsicherheit auf der Grundlage des international verfügbaren Sachverstandes von Experten herauszuarbeiten und deren Einführung in die Praxis der Betreiber und Aufsichtsbehörden zu befördern. Diese Arbeit ist gegenwärtig in vollem Gange. Immer wieder mahnen jedoch Vertreter der UNO, über ein Jahr nach Fukushima die Anstrengungen zur Überwindung der Unfallfolgen und Berücksichtigung der Lehren aus ihnen keinesfalls zu vermindern. So heißt es in einem Pressebericht vom 27.08.2012: „Fast eineinhalb Jahre nach der Atomkatastrophe von Fukushima hat die Internationale Atomenergiebehörde IAEA einen größeren Einsatz bei der Verbesserung der Nuklearsicherheit weltweit gefordert. Auch wenn der Unfall aus den Schlagzeilen verschwunden sei, müssten alle Verantwortlichen ihr Engagement aufrechterhalten, sagte IAEA-Chef Yukiya Amano am Montag in Wien. Der von den Mitgliedstaaten der IAEA im vergangenen Jahr als Reaktion erarbeitete Aktionsplan müsse komplett umgesetzt werden. Es liegt noch viel Arbeit vor uns, und wir dürfen unsere Wachsamkeit nicht verlieren.“ Die Gefahr des „zu schnellen Übergehens zur Normalität wie vor Fukushima“ ist offenbar in einigen Regionen oder Ländern gegeben.

6. Stresstest und verbesserte Sicherheitsstandards für Kernkraftwerke in der EU

Parallel und wechselseitig befördernd mit den Schritten der IAEA begannen auch in den Gremien der Europäischen Union umfangreiche Aktivitäten in Reaktion auf das Unfallgeschehen in Japan: So forderte der Europäische Rat auf maßgebliche Initiative der Bundesregierung am 24./25.03.2011 umfassende Sicherheits- und Risikobewertungen für alle 140 Kernreaktoren in der EU und erteilte der EU-Kommission den Auftrag hierzu, in Zusammenarbeit

mit den maßgeblichen Fachgremien der Union und der Mitgliedsländer, unter Einbeziehung der Betreibergesellschaften. Auf zwei parallelen Pfaden sollten einerseits die technische Sicherheit (safety) und andererseits die Zugangs- und Anschlagssicherheit (security) aller KKW analysiert und bewertet werden. Der Initiative aller 15 EU-Länder mit Kernkraftnutzung schlossen sich die Schweiz und die Ukraine an, so dass sich insgesamt 17 Länder am dreistufigen Stresstest beteiligten.

In der ersten Stufe legten die Betreiberorganisationen, auf der Grundlage der von den europäischen Aufsichtsbehörden vorgegebenen Kriterien und Fragenkataloge, den zuständigen Aufsichtsbehörden Berichte zu den einzelnen Anlagen vor, die von letzteren bis zum 31.12.2011 zu Länderberichten an die EU zusammengefasst und verdichtet wurden. Die zweite Stufe umfasste eine unabhängige gutachterliche Bewertung (peer review) der 17 Länderberichte durch eine unabhängige Gutachterkommission von 70 Experten aus 24 Ländern unter Anleitung und Kontrolle von 8 „Senior Regulatoren". Dieser Prozess umfasste auch Visiten vor Ort zur kritischen Begutachtung der Anlagenbewertungen und Begründung der eigenen, unabhängigen Einschätzung seitens der Gutachter. Die Ergebnisse wurden bis Mai 2012 zum Gesamtbericht an die EU-Kommission zusammengefasst. Im dritten und letzten Schritt fertigte die EU-Kommission mithilfe der zuständigen europäischen Fachgremien (ENSREG und WENRA) und im Austausch mit den zuständigen nationalen Behörden und Aufsichtsgremien (in der Bundesrepublik das Umweltministerium und die RSK) den Abschlussbericht an, in dessen Anlage sich auch sämtliche überarbeiteten Länderberichte befinden.

Im Zentrum des Stresstestes stehen die Fragen, wie sich die einzelnen Anlagen im Falle von Erdbeben oder Überflutungen außerhalb der Auslegungsgrenzen verhalten, wie lange im Extremfall Sicherheitsfunktionen an den Reaktoren und ihren Nebenanlagen aufrecht erhalten werden können und welche Notfallmaßnahmen in solchen Fällen verfügbar sind (vgl. ENSREG 2012).

Welches sind stichpunktartig die Hauptergebnisse dieser umfangreichen, internationalen Initiative:

- Es liegen detaillierte Bewertungen durch unabhängige Experten aus einer nationale Grenzen übergreifenden Sicht für alle KKW in den 17 Ländern vor;
- durch ENSREG werden im Zuge dieses Vorhabens auch einheitliche Richtlinien für die Bewertung von natürlichen Gefahrenquellen und einschlägige Grenzwerte (betreffend Standortwahl, Auslegung, Bau, Be-

trieb, Nuklearhaftung etc.) erarbeitet;
- für jedes KKW werden künftig in regelmäßigen Abständen Sicherheitsreports überarbeitet;
- Maßnahmen zur Sicherung der Integrität des Containments (Druckentlastung auf der Primärseite, Verhinderung von Wasserstoffexplosionen);
- Maßnahmen zur Prävention von Unfällen durch Naturkatastrophen und Begrenzung von deren Folgen (Bunkerung von Sicherheitsausrüstungen, mobile Notfallausrüstungen, Managementzentren für Notfallsituationen, mobile Havarietrupps, grenzüberschreitende Notfallplanungen etc.) wurden herausgearbeitet und dokumentiert.

Im Bericht der EU- Kommission, vorgelegt von Kommissar Günther Oettinger am 04.10.2012, wird generell ein hohes Sicherheitsniveau bei allen 145 europäischen KKW festgestellt, das keine sofortigen Abschaltungen erforderlich macht. Zugleich sind jedoch zahlreiche Mängel und Sicherheitslükken aufgedeckt worden, so dass Maßnahmen an vielen KKW empfohlen werden: Hinsichtlich Erdbeben- und Überflutungsgefahr erfüllen 54 bzw. 62 Reaktoren nicht die aktuellen Standards der Risikoabschätzung. An 32 Reaktoren gibt es keine Systeme zur gefilterten Containment-Druckentlastung. Bei 81 KKW ist die Lagerung von Notfallausrüstung für schwere Unfälle nicht ausreichend gesichert. Für 24 Reaktoren ist kein Ersatz-Kontrollraum vorhanden. Der Nachrüstungsbedarf pro Reaktor liegt im Kostenbereich von 30 bis 200 Millionen Euro, insgesamt für die Kernkraftwerke in der EU summiert sich der Finanzbedarf auf 10 bis 25 Mrd. Euro!

Unterschiedlich fallen die Bewertungen der KKW in den einzelnen Ländern aus: In der Schweiz wurden keine Mängel bei Sicherheitsausrüstung und Organisation festgestellt, umfassende Erdbeben-Gefährdungsanalysen liegen vor, mehrfache und unabhängige Systeme für Nachkühlung und Stromversorgung sind vorhanden. Bei deutschen KKW wurden keine Mängel bei Kühlwasser, Stromversorgung und Notfallmaßnahmen festgestellt. Die installierten Erdbeben-Warnsysteme müssen teilweise nachgebessert oder nachgerüstet werden, insbesondere bei KKW in Norddeutschland. Kritisch ist vermerkt, dass die IAEA-Leitlinien für schwere Unfälle bisher nicht umgesetzt worden sind. Zwei Reaktoren in Finnland und Schweden haben schwere Mängel hinsichtlich zu kurzer Reaktionszeit der Bedienmannschaft nach einem kompletten Stromausfall. Französische KKW schneiden generell schlecht ab – fehlende oder ungenügende Erdbeben-Messgeräte, nicht sichere Lagerung von Unfallausrüstungen sowie Mängel bei der Prüfung von Erdbe-

ben- und Flutgefahren sind die hauptsächlichen Kritikpunkte (vgl. Spiegel 2012).

Die umfassende Implementierung der genannten Schritte zur Erhöhung der Nuklearsicherheit und deren Überwachung stehen nun auch auf der Tagesordnung der europäischen Ebene, sie sind nicht mehr alleinige Angelegenheit eines einzelnen Mitgliedslandes. Bis Ende 2012 sollen die nationalen Aufsichtsbehörden ihre Aktions- und Zeitpläne zur Umsetzung vorlegen. Diese werden in einem erneuten Peer-review-Verfahren überprüft, und bis zum Juni 2014 soll ein erneuter Bericht durch die EU-Kommission über die erfolgte Umsetzung vorgelegt werden. Parallel dazu sollen Anfang 2013 neue EU-Richtlinien über nukleare Sicherheit vorliegen. Insgesamt strebt die EU höhere Kompetenzen auf dem Gebiet der Nuklearsicherheit gegenüber den nationalen Aufsichtsbehörden an. Auch auf diesem Gebiet wird es darauf ankommen, die gezogenen richtigen Lehren und Schlussfolgerungen aus dem Reaktorunfall in die dauerhaft festgeschriebene Praxis der Betreiber von Nuklearanlagen zu überführen, sie weder aufweichen noch versanden zu lassen (vgl. BDIP 2012; NFS 2012).

7. Ausstieg aus der Kernenergie – ein deutsche Sonderweg

Die wesentlichen Entscheidungen in der Bundesrepublik Deutschland nach dem Unfall von Fukushima sollen hier noch einmal in Erinnerung gerufen werden: Bereits wenige Tage nach dem Unfall, am 14./15.03.2011, fiel der Regierungsbeschluss über ein dreimonatiges Moratorium für die beschlossene Laufzeitverlängerung und sowie die Abschaltung aller älteren KKW. Am 16.03.2011 fasste der Bundestag den Beschluss, eine Sicherheitsüberprüfung für alle deutschen KKW durchzuführen. Der Bundes-Umweltminister beauftragt hierzu die RSK. Der Abschlussbericht der RSK, ausgearbeitet gemeinsam mit der GRS, dem TÜV, dem Ökoinstitut Darmstadt und anderen kompetenten Partnern lag am 16.05.2011 vor. Das Fazit des Berichts lautet: Die deutschen KKW sind ausgelegt gegen 1.000-jährige Überflutung und Erdbeben. Die Stromversorgung ist robuster als die von Fukushima, Reserven bestehen hinsichtlich der Erbebenauslegung und gegen 10.000-jähriges Hochwasser. Es wurden keine Sicherheitsunterschiede zwischen älteren und jüngeren KKW festgestellt (vgl. RSK 2011).

Parallel und unabhängig von der Sicherheitsüberprüfung erfolgte am 22.03.2011 der Regierungsauftrag an eine eigens berufene Ethikkommission, die Machbarkeit des Ausstiegs aus der Kernenergienutzung zu prüfen. Deren Abschlussbericht am 30.05.2011 erklärte den Ausstieg innerhalb eines Jahr-

zehnts für möglich und betonte, dass Deutschland eine Vorreiterrolle beim Atomausstieg spielen sollte. Die Möglichkeit des Scheiterns wird allerdings eingeräumt, ebenso wie sich daraus ergebende Konsequenzen. Bemerkenswert ist, dass dieser Bericht keinerlei Bezug zum Bericht der RSK enthält! Auf dieser Grundlage fällt am 06.06.2011 der Regierungsbeschluss über die Eckpunkte zur Energiewende. Der gesetzliche Vollzug erfolgt am 31.07.2011 im Rahmen der 13. Novelle zum Atomgesetz: Rücknahme der Laufzeitverlängerung von 2010, dauerhafte Abschaltung der vom Moratorium betroffenen 8 KKW sowie schrittweise Abschaltung aller verbliebenen 9 KKW bis zum Jahr 2022.

8. Zu einigen übergreifenden Aspekten und Fragen nach der Katastrophe

Zweifellos bedeutet der desaströse Reaktorunfall von Fukushima infolge einer Naturkatastrophe einen tiefen Einschnitt in der bisherigen Nutzung der Kernenergie nicht nur in Japan, sondern für die Energiepolitik der Staaten weltweit. Als diametral entgegengesetzte Alternativen für die künftige Energiepolitik kommen infrage: entweder der konsequente Ausstieg aus der Nutzung von Kernkraft zur Elektroenergieerzeugung oder deren Weiterführung und Ausbau auf der Grundlage einer vertieften Durchdringung aller sicherheitsrelevanten Risiken unter Nutzung neuer Erkenntnisse von Wissenschaft und Forschung. Auf Beschluss der Bundesregierung beschreitet Deutschland den ersteren Weg, auch Japan hatte sich aus naheliegendem Grund zunächst dafür entschieden, später jedoch den vollständigen Ausstieg wieder infrage gestellt. Die meisten anderen Länder halten bisher an der Kernenergie fest und verbinden zur Begründung dafür zu Recht auch das Argument der Klimaschonung infolge verringerter Treibhausgasemission. Einige Fragen bleiben offen: „Gibt es eine ausreichende, risikolose technologische Grundlage der Energiegewinnung ohne fossile Brennstoffe und ohne Kernenergie, welche die nachhaltige Entwicklung einer Industriegesellschaft auf der Erde, inklusive des wachsenden Energiebedarfs der aufstrebenden Regionen, in der Zukunft ermöglicht?“, „Wie gut kennen die Menschen die tatsächlich Risiken alternativer, nicht nuklearer Technologieentwicklungen, wie viel sind sie bereit zu tragen und zu welchem Preis?“, „Bewirkt der Reaktorunfall von Fukushima den Beginn des globalen Ausstiegs aus der Nutzung der Technologie der Kernspaltung, die infolge der Entstehung radioaktiver Spaltprodukte und deren unvermeidliche Nachwärmefreisetzung so große Schwierigkeiten für die Techniksicherheit mit sich bringt, oder werden in einigen Jahrzehnten Tsunami und Unfall von Fukushima als Beispiel dafür gesehen, wie eine hoch

entwickelte Industriegesellschaft selbst schwerste Natur- und Technik-Katastrophen beherrscht und daraus langfristig gestärkt hervorgehen kann?".

Es ist nicht nur in Deutschland eine Zunahme der gesamtgesellschaftlichen und politischen Relevanz der Energiestrategie festzustellen – das Thema gewinnt wahlentscheidende Bedeutung in den Demokratien. Ein Aspekt dabei ist die Durchsetzung gesamtgesellschaftlicher Interessen gegenüber den partiellen ökonomischen Interessen von Kraftwerksbetreibern und deren Verbänden: Kann die Marktwirtschaft das leisten? Einerseits hat die Bevölkerung, beispielsweise mithilfe des Internets, zunehmend stärkere Hebel zum Artikulieren und zur Durchsetzung ihrer Interessen in der Hand. Andererseits finden solide technologisch-wissenschaftliche Erkenntnisse gegenüber halbwissenschaftlichem Medienspektakel zunehmend weniger Beachtung in der öffentlichen Wahrnehmung. Zugespitzt könnte man die Frage formulieren: „Was bestimmt stärker die Politik regierender Parteien – erfolgversprechende Wahlkampfstrategien unter Nutzung medienwirksamer Vorurteile oder die nüchterne Analyse fundierter naturwissenschaftlich-technischer Erkenntnisse?".

Ein weiteres Problem gewinnt durch Fukushima an Aktualität: Es handelt sich um die Abwägung von Sicherheitsrisiken der Technik bei seltenen, wahrscheinlich nie eintretenden Naturkatastrophen gegenüber der akut notwendigen Reduzierung der Emission von Treibhausgas und damit der Einhaltung der Ziele zur Stabilisierung des Erdklimas. Wo liegt das Optimum bei Entscheidungen für oder gegen den künftigen Einsatz von Nukleartechnologie?

Gleichermaßen kann eine Zunahme der internationalen bis hin zur globalen Relevanz energiepolitischer Probleme festgestellt werden. Insbesondere zur Verhütung von und Hilfe in Notfällen gewinnt die Durchsetzung verbindlicher zwischenstaatlicher Regularien zur Sicherheitstechnik gegenüber partiellen Souveränitätsansprüchen einzelner Länder immer mehr an Bedeutung. Gelegentlich wird infrage gestellt, ob das bestehende System der UNO einen ausreichenden Rahmen dafür bietet. Es ist aber bisher der einzige global funktionierende Rahmen dafür, und Fukushima zeigt auch: Auf dem Wege der gleichberechtigten Zusammenarbeit von Fachleuten in internationalen Organisationen, wie der IAEA, entsteht weltweit gemeinschaftliches Verantwortungsbewusstsein und Handeln, insbesondere auch zu Problemen der Techniksicherheit. Regionale Gremien, wie die Organisationen zur Nuklearsicherheit in der EU, die ihre spezifischen Aktivitäten in Einklang mit denen der IAEA entfalten oder auch branchenspezifische internationale Gremien,

wie die WANO, untersetzen und ergänzen das Handeln in ihren jeweiligen Verantwortungsbereichen im Interesse der Techniksicherheit. Zum kontinuierlichen Ausbau dieses bewährten Systems internationaler Kooperation von Experten im Interesse erhöhter Sicherheitskultur gibt es keine vernünftige Alternative. Ihr wird auch eine optimierende Rolle bei der schrittweisen Lösung des Konflikts zwischen den Sicherheitsrisiken von Nuklearanlagen bei Eintreten von Naturkatastrophen einerseits und der notwendigen Reduzierung der Emission von Treibhausgasen andererseits zukommen.

In diesem Sinne bleibt die Techniksicherheit im weitesten Sinne auch in Zukunft ein spannendes Feld der Auseinandersetzung und Kompromiss-Suche sowohl bei der Verteilung wissenschaftlich-technischer Ressourcen wie auch bei der Wahrnehmung ökonomischer, politischer und diplomatischer Interessen.

Verwendete Abkürzungen

ENSREG – European Nuclear Safety Regulators‘ Group (Expertengremium aus Vertretern der Genehmigungsbehörden der EU-Länder, welches die EU-Kommission berät)

GRS – Gesellschaft für Anlagen- und Reaktorsicherheit

IAEA – International Atomic Energy Agency (Spezialorganisation der UNO für Atomenergie)

RSK – Reaktorsicherheits-Kommission (Beratungsgremium des Ministers für Umwelt zu Fragen der Reaktorsicherheit)

WANO – World Association of Nuclear Operators (weltweite Organisation der Betreiber von KKW)

WENRA – Western European Nuclear Safety Regulators`Association (Arbeitsgemeinschaft der westeuropäischen kerntechnischen Aufsichts- und Genehmigungsbehörden)

Literatur

AREVA GmbH (Hg.) (2012): Kernenergie nach Fukushima – Lehren und Konsequenzen. Erlangen, März (AREVA-argumente) – URL: http://www.areva.com/DE/areva-deutschland-985/argumente-Gruppe AREVA [03.05.2013]

ATF – Deutsches Atomforum e.V. Berlin (2012): Der Reaktorunfall von Fukushima Daiichi – Folge fehlerhafter Auslegung und unzureichender Sicherheitstechnik. – URL: http://www.kernenergie.de/kernenergie-wAssets/docs/service/024reaktorunfall_fukushima.pdf [27.04.2013]

Bericht (2012): EU-Atomstrom unterliegt den strengsten Sicherheitsauflagen der Welt. Bericht der EU-Kommission zu den Stresstests der Atomkraftwerke in der

Europäischen Union, 4.10.2012. In: Blätter für Deutsche und Internationale Politik. – URL: http://www.blaetter.de/archiv/jahrgaenge/dokumente/%C2%BBeu-atomstrom-unterliegt-den-strengsten-sicherheitsauflagen-der-welt%C2%AB [27.04.2013]

ENSI – Eidgenössisches Nuklearsicherheitsinspektorat (2011): Ablauf Fukushima 11032011 – Ereignisabläufe Fukushima Daiichi und Fukushima Dairi infolge des Tohoku-Chihou-Taiheiyou-Oki-Erdbebens vom 11.03.2011. Bericht ENSI-AN-7746 vom 16.12.2011. Brugg

ENSREG– European Nuclear Safety Regulators Group (2012a): Peer Review Report "Stress Tests Performed on European Nuclear Power Plants". – URL: http://www.ENSREG.de [25.04.2012]

ENSREG– European Nuclear Safety Regulators Group (2012b): Joint Statement of ENSREG and the European Commission on Stress Tests and Peer Review Process. – URL: http://www.ensreg.eu/node/389 [26.04.2012]

GRS – Gesellschaft für Anlagen- und Reaktorsicherheit (2011): Fukushima Daiichi 11. März 2011 – Unfallablauf, radiologische Folgen. Bericht GRS-S-51. – URL: http://www.grs.de/publication/GRS-S-51 (siehe auch 2., überarb. Aufl.: GRS-S-53, 2013) [03.05.2013]

GRS – Gesellschaft für Anlagen- und Reaktorsicherheit (2012): Erläuterungen zum Stresstest deutscher KKW vom 24.11.12. – URL: http://www.grs.de/de/print/1618 [03.05.2013]

IAEA – International Atomic Energy Agency (2008): INES – THE INTERNATIONAL NUCLEAR AND RADIOLOGICAL EVENT SCALE USER'S MANUAL. – URL: http://www-pub.iaea.org/MTCD/publications/PDF/INES-2009_web.pdf [03.05.2013]

IAEA – International Atomic Energy Agency (2011a): IAEA Action Plan on Nuclear Safety. Vienna, September. – URL: http://www.iaea.org/newscenter/focus/actionplan [03.05.2013]

IAEA – International Atomic Energy Agency (2011b): Fukushima Daiichi Status Report. Vienna, 04.11. – URL: http://www.iaea.org/Fukushima Daiichi Status Reports [03.05.2013]

IAEA – International Atomic Energy Agency (2011c): Fukushima Daiichi Status Report. Vienna, 10.11. – URL: http://www.iaea.org/Fukushima Daiichi Status Reports [03.05.2013]

IAEA – International Atomic Energy Agency (2011d): IAEA International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great East Japan Earthquake and Tsunami. 16.06. – URL: http://www-pub.iaea.org/MTCD/PDFplus/2011/cn200_Final-Fukushima-Mission_Report.pdf [03.05.2013]

IAEA – International Atomic Energy Agency (2012): Fukushima Daiichi Status Report. Vienna, 31.08. URL: http://www.iaea.org/Fukushima Daiichi Status Reports [03.05.2013]

JAIF – Japan Atomic Industrial Forum Inc (2011): Information on Status of Nuclear Power Plants in Fukushima. 01.06. –
URL: http://www.jaif.or.jp/english/fukushima/plantstatus201106.html [03.05.2013]

JPG – Japanese Government (2011): Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety – The Accident at TEPCO's Fukushima Nuclear Power Stations. 07.06. –
URL: www.iaea.org/newscenter/Focus/fukushima/japan-report [03.05.2013]

Kuczera, B. (2011): Das schwere Tohoku-Seebeben in Japan und die Auswirkungen auf das Kernkraftwerk Fukushima-Daiichi. In: atw – Internationale Zeitschrift für Kernenergie, Jg. 56, H. 4/5, S. 2-9. –
URL: http://www.kernenergie.de/kernenergie-wAssets/docs/fachzeitschrift-atw/2011/atw2011_05_kuczera_fukushima.pdf [27.04.2013]

NFS – Nuklearforum Schweiz (Hg.) (2012): EU-Stresstest: gut, aber Verbesserungen nötig. Bericht vom 04.10. – URL: http://www.nuklearforum.ch/de/aktuell/e-bulletin/eu-stresstest-gut-aber-weitere-verbesserungen-noetig [27.04.213]

RSK – Reaktorsicherheitskommission (Hg.) 2011: RSK-Stellungnahme „Anlagenspezifische Sicherheitsüberprüfung (RSK-SÜ) deutscher Kernkraftwerke unter Berücksichtigung der Ereignisse in Fukushima-I (Japan)". 437. Sitzung der RSK, 11.-14.05.2011. –
URL: http://www.bmu.de/fileadmin/bmu-import/files/pdfs/allgemein/application/pdf/sicherheitsueberpruefung_stellungnahme_rsk.pdf [27.04.2013]

Spiegel Online (2012): EU-Stresstest – Sicherheitsmängel bei zwölf deutschen AKW. Bericht vom 01.10. – URL: http://www.spiegel.de/wissenschaft/technik/eu-stresstest-sicherheitsluecken-bei-zwoelf-deutschen-akw-a-858881.html [27.04.2013]

TEPCO (2012): Mid-and-long-Term Roadmap towards the Decommissioning of Fukushima Daiichi. Nuclear Power Station Units 1-4. 25.01. –
URL: http://www.tepco.co.jp/en/nu/fukushima-np/roadmap [03.05.2013]

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 79–98*

Ernst-Otto Reher

Überwachung und Qualitätssicherung fluider, strukturierter Erzeugnisse aus Produktionsanlagen, dargestellt am Beispiel der Kunststofftechnologie

1. Zur Überwachung und Qualitätssicherung der Erzeugnisse aus Produktionsanlagen der stoffwandelnden Industrie

Die Produktionsanlagen der Materialtechnologien müssen mit einer Vielzahl von Eigenarten der zu wandelnden Stoffe und in ihnen ablaufenden Prozesse fertig werden. Eine repräsentative Aufzählung der Kennzeichen derartiger Anlagen und Stoffe ist in der Tabelle 1 zusammengestellt. Die Merkmale der Anlagen und die in ihnen zu wandelnden Stoffe haben, wie wir später konkret sehen werden, einen großen Einfluss auf die Verfahrens- und Geräteentwicklung zur Überwachung und Produktqualitätssicherung.

Die Qualität wird definiert als „Güte, Beschaffenheit, Eigenschaft einer Sache, Gesamtheit der Eigenschaften von Erzeugnissen, die den Grad ihrer Eignung für den vorgesehenen Verwendungszweck bestimmen“ (Universallexikon 1988). Die Qualitätssicherung erfolgt durch Maßnahmen in Form von Modellen, Konzeptionen, Normen, Grenzwerten, Gesetzen, Techniken u.v.m., die alle der Qualitätssicherung dienen (s. Abbildung 1). Dabei erfassen die Maßnahmen den gesamten Reproduktionsprozess und alle Hierarchieebenen der technologischen Artefakte und Produkte, die dort entstehen (z.B. Reaktor, Mühle, Filter, Trockner, Anlage, Betrieb usw.). Eingebunden zur Lösung der Produktsicherung sind alle Wissenschaftsdisziplinen (s. Abbildung 2). Materialwissenschaftler entwickeln Verfahren und Laborgeräte, um Struktur-Eigenschaftsbeziehungen zu erforschen. Ingenieure entwickeln dazu entsprechende Verfahren und Geräte unter Beachtung der Eigenarten der Ausrüstungen (s. Tabelle 1) und für den Einsatz in den Artefakten zur Überwachung und Qualitätssicherung der Erzeugnisse.

Anlagen allgemein
Einstrang(-Produkt)-Anlagen, Mehrproduktanlagen, Kontinuierliche, halbkontinuierliche, diskontinuierliche Anlagen, Hochdruck-, Niederdruck-, Vakuum-Anlagen, Spezialanlagen
Anlagenkennzeichnungen nach
• Gefahrenklassen • Erzeugnissen (Chemikalien, Lebensmittel, Pharmaka, Kosmetika, Kleidung u.a.) • Raum-Zeit-Ausbeuten • Prozess-Schaltungen • Koppelprodukten • Hygieneanforderungen • Einsatzgebieten (ortsgebundene, bewegliche) • geometrischen Abmessungen (Mikro – Makro) • Vorgangstechnologien (Verfahrens-, Verarbeitungs-, Fertigungstechnik) • Temperaturbedingungen u.v.m.
Stoffkennzeichnung nach
• Aggregatzustand • Gefahrenklasse • Toxikologie/Giftigkeit • Aggressivität der Medien • Explosionsfähigkeit • Erosionsfähigkeit • Fließfähigkeit (rheologischer Zustand) • Dispersitätszustand (fein, grobkörnig) • Färbung (durchsichtig, trübe) u.v.m.

Tabelle 1: Kennzeichnung von Produktionsanlagen und Stoffen der Stoffwirtschaft
Eigene Darstellung

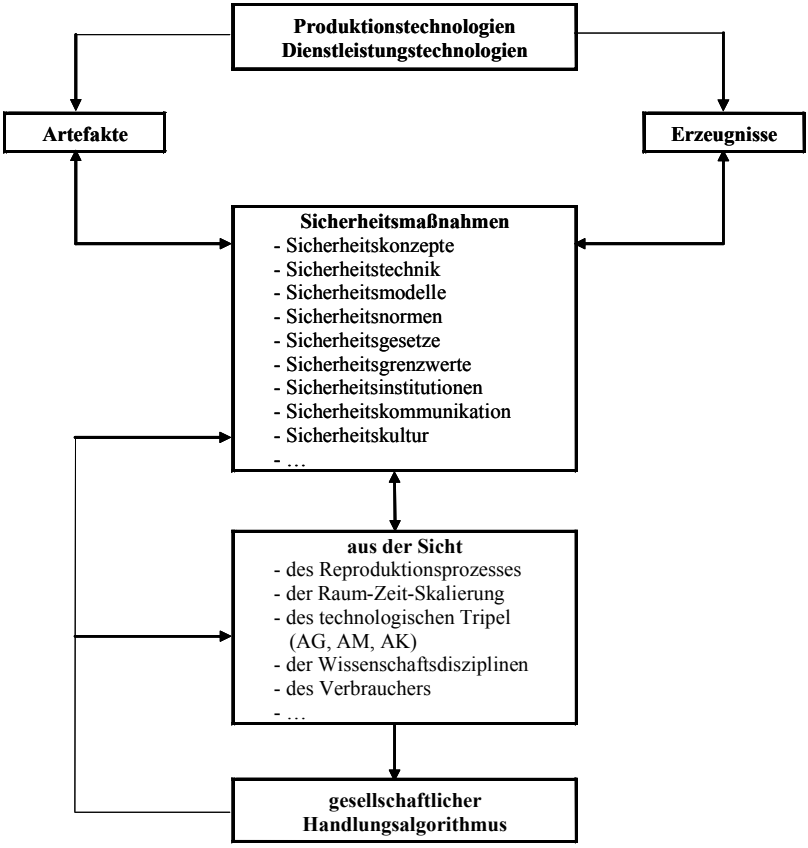


Abbildung 1: Maßnahmen zur Qualitätssicherung
Eigene Darstellung

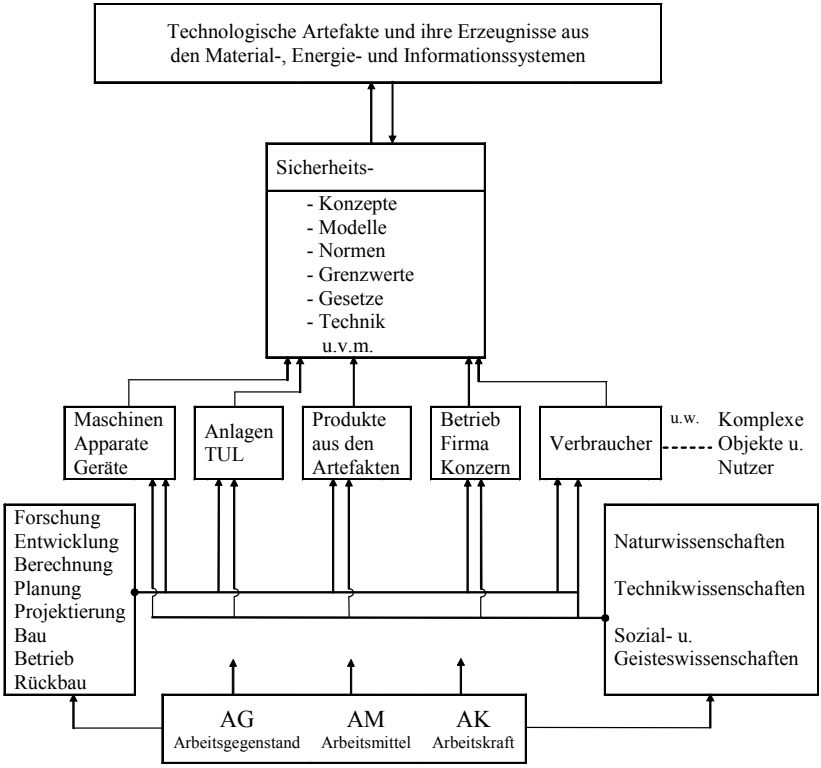


Abbildung 2: Multidimensionale Entwicklung und Bereitstellung von Maßnahmen zur Sicherheit in technologischen Artefakten und für Produkte
Eigene Darstellung

Die gewonnenen Daten aus den Ausrüstungen (Maschinen, Apparate, Anlagen) dienen außerdem

- zur Steuerung der Ausrüstungen (vgl. z.B. Fritz/Stöhrer 1986);
- der Komplettierung der mathematischen Modelle für die Erzeugnisweiterverarbeitung oder Anwendungstechnik (vgl. z.B. Hartmann/Reher 2009).

Sozial- und Geisteswissenschaftler erarbeiten Grenzwerte, Normen und sind bei den Gesetzesvorbereitungen involviert.

Am Beispiel der Kunststofftechnologie soll später der Entwicklungsprozess der Prozesstechnik zur Überwachung und Qualitätssicherung und damit zur Prozess-Steuerung von Polymerisationsreaktoren für Polyethylene und Polypropylene im Detail dargestellt werden. In Abbildung 3 ist ein allgemei-

ner Ablaufvorgang zur Entwicklungs- und Nutzungsfolge der Prozessmesstechnik zur Produktqualitätssicherung dargestellt.

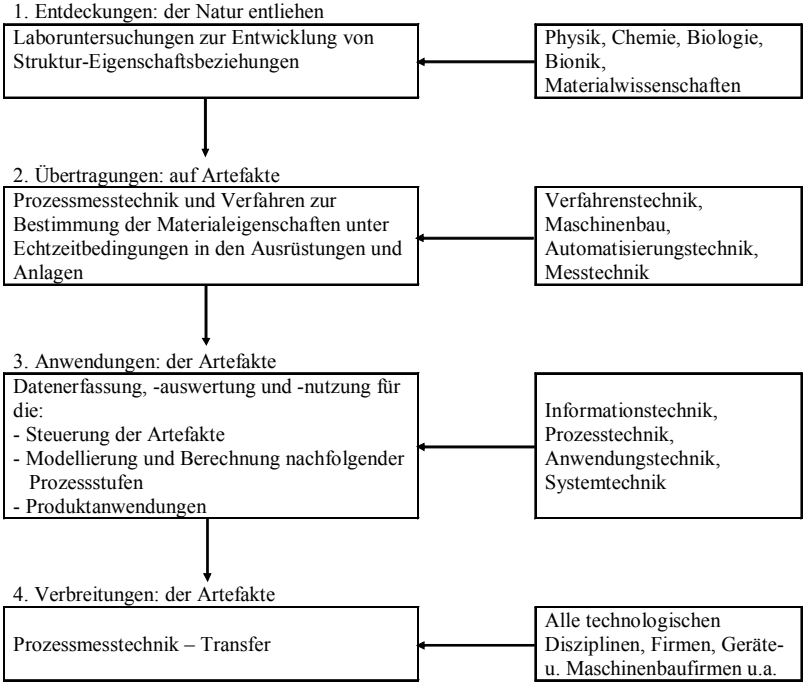


Abbildung 3: Entwicklungs- und Nutzungsfolge der Prozessmesstechnik zur Produktqualitätssicherung
Eigene Darstellung

Die Labormessverfahren sind die Grundlage für die Bereitstellung der Prozessmesstechnik. Die Entwicklung der Prozessmesstechnik ist daher durchaus keine triviale Aufgabenstellung, wenn man die in der Tabelle 1 dargestellten Eigenarten der Artefakte beachten muss. Einige Merkmale, wie Druck, Temperatur u.v.a. sind relativ leicht realisierbar. Komplizierter ist die Probennahme bzw. Probenbereitstellung im Echtzeitbetrieb aus kontinuierlich arbeitenden Ausrüstungen bzw. Anlagen. Dazu sind in der Regel besondere konstruktive Lösungen der Prozessmesstechnik erforderlich. Auch der Messvorgang und die Datenauswertung und Bereitstellung, z.B. zur Steuerung der Ausrüstung oder Anlage, muss im Echtzeitbetrieb erfolgen, da sonst zu viel Mangelware (Ausschuss) produziert wird. Die Labormesstechnik

bzw. Prozessmesstechnik zur Qualitätssicherung ist ausreichend, wenn die Bedingung für diskontinuierliche Prozesse gilt:

Labormesszeit << Prozesszeit.

Für einige Prozesse der Kunststofftechnologie wird diese Bedingung auch erfüllt, jedoch nicht für alle. Für kontinuierliche Prozesse dagegen muss mindestens die folgende Bedingung erfüllt sein:

Messzeit ≤ Prozesszeit,

da ansonsten zu viel unkontrollierte Produkte die Anlage verlassen.

Industriebereich	Beispiele Produkte: strukturierte Fluide
Kunststoffindustrie	Schmelzen, Lösungen, Dispersionen
Lebensmittelindustrie	Schokolade, Joghurt, Käse, Sahne, Sirup, Honig, Teige, Schäume, Quark, Fette, Kaugummibasen, Wurst
Pharmaindustrie	Creme, Salben, Lösungen, Beschichtungsfluide, Augentropfen, Nasenspray
Bau- und Keramikindustrie, Glasindustrie	Betonsuspensionen, Keramik-Schlicker, Porzellan-Pasten, Tonsuspensionen, Glasschmelzen
Farben- und Lackindustrie	Pigmentpasten, Farben, Lacke, Anstrichstoffe, Kugelschreiberpasten
Agrarindustrie	Biosuspensionen, Gülle, Futtermittel
Aufbereitungsindustrie	Bohrschlämme, Erdöl, Asphalt, Kohlesuspensionen, Erzsuspensionen, Schäume, Abwasserschlämme
Medizintechnik	Blut, Speichel, Synovialflüssigkeiten, Harn, Kot, Eiter, Zahnersatzmassen
Biotechnologie	Dispersionen: Fluid-Fluid, Fluid-Fest, Fluid-Gas
Nanotechnologie	s. Biotechnologie
Fahrzeugindustrie	Treibstoffe, Schmierstoffe, Bremsflüssigkeit, Kühlflüssigkeit, Hydraulik

Charakteristischer Zusammenhang:
Rheologie = f(Struktur, Eigenschaften, Verarbeitbarkeit, Anwendbarkeit)

Abbildung 4: Strukturierte Fluide in Technologie- und Lebensbereichen
Eigene Darstellung

Die Vielfalt der strukturierten Fluide in der Stoffwirtschaft ist sehr groß und in Abbildung 4 dargestellt.

2. Überwachung und Qualitätssicherung der Kunststofferzeugnisse

Die Qualitätssicherung der Kunststofferzeugnisse verläuft im Wesentlichen über den viskoelastischen Fluidzustand der Kunststoffschmelze. Er ist auch verantwortlich für die Verarbeitbarkeit der Schmelze.

Dieser Schmelzezustand wird in den Polymerisationsanlagen der Kunststoffindustrie realisiert und wirkt sich später in den Verarbeitungsprozessen der Kunststoffe und in der Anwendung der Erzeugnisse aus. Der viskoelastische Fluidzustand der Kunststoffschmelze wird durch die molekulare Struktur der Polymeren bestimmt. Da aber die molekulare Strukturbestimmung (mittlere Molmasse $\overline{M}_w$, Molekulargewichtsverteilungsbreite oder Polydispersität M_w/M_n, Molekulargewichtsverteilung $M(d)$) sehr zeitaufwendig ist, kann sie in den Kunststoffanlagen zur Echtzeitqualitätssicherung nicht angewendet werden. In modernen Polymerisationsanlagen werden Millionen Jahrestonnen produziert, d.h. 100 und mehr t/h fallen an. Die Dauer der Bestimmung der molekularen Daten im Labor beträgt aber mehrere Stunden. Eine Echtzeitbestimmung der Kunststoffschmelzen in den Anlagen ist somit ausgeschlossen. In diesem Falle werden „Ersatzgrößen“ gefordert, die im Echtzeitbetrieb ermittelt werden können und einen Zusammenhang zur molekularen Struktur gewährleisten (s. Tabelle 1 und Abbildung 2).

Rheologische Kennwerte und Funktionen sind geeignet, diese „Ersatzfunktion“ zu übernehmen, zumal diese Daten auch für die Prozessmodelle der Verarbeitungsprozesse und Erzeugnisanwendungen relevant sind und dort auch ihre weitere Anwendung finden.

2.1 Phase der rheologischen On-Line-Bestimmung zur Qualitätssicherung von Kunststoffen

Laboruntersuchungen zur Bestimmung des Schmelzindexes (MVR oder MFR) konnten relativ schnell durchgeführt werden (½ bis 1 Stunde). Diese Daten waren international standardisiert worden und galten als Qualitätsmerkmal zur Produktabgabe an den Verarbeiter. Der Schmelzindex wird mit zertifizierten Geräten im Labor unter definierten Bedingungen gemessen. Er stellt eine Durchflussmenge der Schmelze durch eine genormte Düse (kurze Düse: $^{L}/_{D} = 3{,}81$) bei gegebener Temperatur und Gewichtsbelastung eines Stempels dar. Auf Grund der geometrischen Gegebenheiten des Laborgerätes stellt der

Schmelzindex eine „viskoelastische Kenngröße“ der Schmelze dar. Da in der Regel nur eine Kenngröße ermittelt wird, die aber für den Verarbeitungsprozess nicht repräsentativ und somit untauglich ist, auch in keinem Prozessmodell Verwendung finden kann, mussten andere Wege gegangen werden zur Qualitätssicherung, auf die später noch eingegangen wird. Trotzdem wurde versucht, ein Verfahren und dazugehörige Ausrüstungen zu entwickeln, um den Schmelzindex im On-Line-Betrieb in den Polymerisationsanlagen der Kunststoffindustrie zu ermitteln (vgl. Göttfert/Reher 1998a).

Der Grund dafür war, dass der Schmelzindex eine standardisierte Kenngröße ist, die international in der Praxis gerätetechnisch und technologisch eingeführt war und noch ist. Eine aktuelle erweiterte und verbesserte gerätetechnische und verfahrenstechnische Lösung zur Bestimmung des Schmelzindexes im On-Line-Betrieb der Anlage existiert (vgl. Reher/Göttfert 2000) und wurde auch erfolgreich getestet, aber nicht weiter verfolgt, da die zweite Phase der On-Line-Kapillar-Rheometrie Erfolg versprechender war und auch ist.

Ein weiteres Verfahren der ersten Phase ist die Bestimmung des Staudinger-Indexes $[\eta]$. Er ist definiert als

$$[\eta] = \lim_{\substack{c \to 0 \\ \dot{\gamma} \to 0}} \frac{\eta - \eta_s}{\eta_s c} = \frac{\eta_{spez}}{c} \tag{1}$$

und wird mit dem Zimm-Crothers-Viskosimeter bestimmt (vgl. Kulicke 1986). Der große Vorteil des Staudinger-Indexes ist, dass er folgende Strukturabhängigkeiten identifiziert:

$$[\eta] \sim \overline{M}_w{}^a \tag{2}$$

mit (vgl. Holzmüller/Altenburg 1961)

a = 0	massive Kugeln;
a = 0,5	undurchspültes Knäuel;
a = 0,5-1	teilweise durchspültes Knäuel;
a = 1	voll durchspültes Knäuel;
a = 2	starre Stäbchen.

Vom Autor wurde der Zusammenhang mit der Nullviskosität (η_0) formuliert (vgl. Reher 2000):

$$\eta_0 \sim [\eta]^{\frac{3,4-3,5}{a}} \tag{3}$$

und von Jens Hepperle, Helmut Münstedt, Peter K. Haug und Claus D. Eisenbach für 13 Typen *branched polystyrenes* bestätigt mit a = 0,7096 und K = 1,08 10^{-4} (vgl. Hepperle et al. 2005), so dass Beziehung (3) sich wie folgt ergibt:

$$\eta_0 = 1{,}08 \cdot 10^{-4}\ [\eta]^{4,79-4,93}.$$

Erst durch den Zusammenhang (3) wurde möglich, den Staudinger-Index für die On-Line-Rheometrie anzuwenden. Wie später noch gezeigt wird, lässt sich η_0 leicht aus rheometrischen Daten bestimmen. Zuvor war der zeitliche Aufwand zur Bestimmung von $\overline{M}_w$ oder $[\eta]$ für On-Line-Verfahren zu groß.

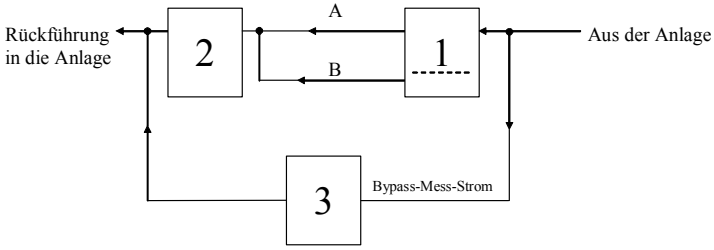
2.2 Phase der rheologischen On-Line-Bestimmung zur Qualitätssicherung von Kunststoffen

Diese Phase ist gekennzeichnet durch die Entwicklung und Einführung von Ein- und Mehrkapillar-Rheometern in die Prozesstechnik (vgl. Reher et al. 2002). Dadurch konnten alle bisher erwähnten Verfahren erst einmal realisiert werden. Die mittlere Verweilzeit (Ansprechzeit) des Materials konnte durch folgende abgeleitete Gleichung

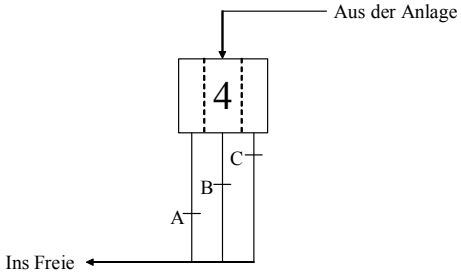
$$\frac{t_{Ansprechzeit}}{t_{Messkanal}} = 1 + \frac{V_{Adapter}}{V_{Messkanal}} \cdot \frac{1}{1 + \frac{\dot{V}_{Umlaufstrom}}{\dot{V}_{Messkanal}}} \tag{4}$$

im Gerät bestimmt und durch die Gerätekonstruktion beeinflusst werden, um im variablen Echtzeitbetrieb die Messung durchführen zu können (s. Abbildung 5). Mit dieser neuen Gerätetechnik war es erstmals möglich, verschiedene rheologische Betriebsweisen zu realisieren. Die verbreitetste Betriebsweise ist:

1. Bestimmung der Viskositätsfunktion η (η_0, $\dot{\gamma}$, T) in einem größtmöglichen Variablenbereich (s. Abbildung 6).
2. Bestimmung des elastischen Einlaufdruckes des Materials in die Kapillaren (Bagley-Einlaufdruck (P_E ($\dot{\gamma}$, M_w/M_n)) (s. Abbildung 6).



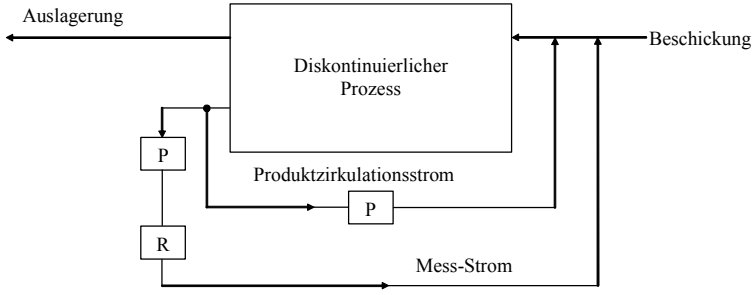
a) Geschlossene On-Line-Rheometer



b) Offene On-Line-Rheometer

A, B, C Mess-Strecken: Kapillaren oder Schlitze mit Druckaufnehmern
1-4: Dosierpumpen

Abbildung 5a: On-Line-Rheometer für kontinuierliche Prozessführung
Eigene Darstellung



(R) – Rheometer, (P) – Pumpen

Abbildung 5b: Diskontinuierlicher Prozess mit rheologischer Prozesskontrolle
Eigene Darstellung

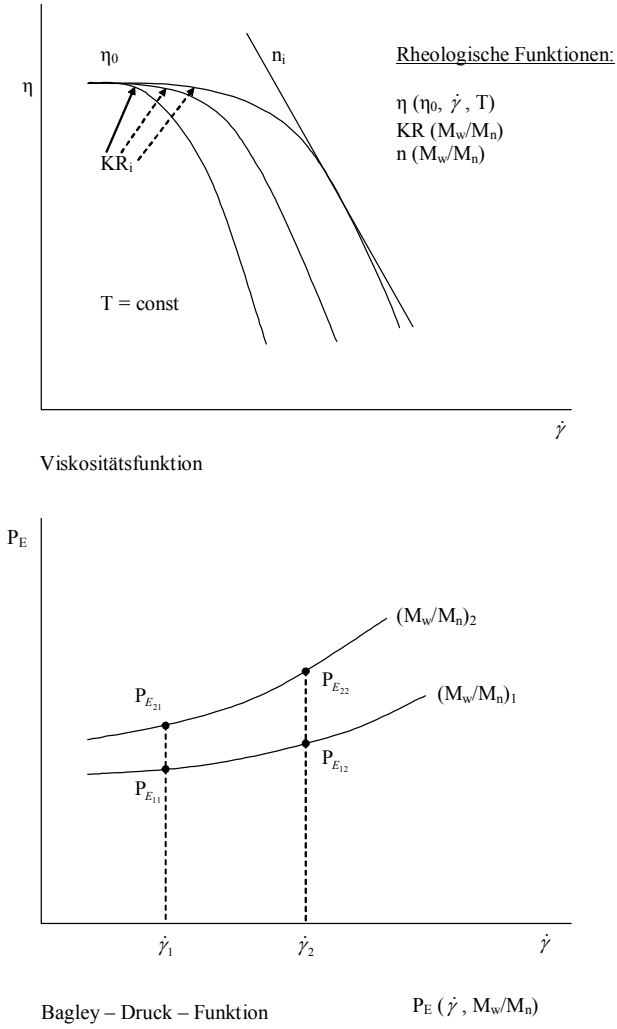


Abbildung 6: Rheologische Funktionen, gewonnen aus On-Line-rheometrischen Messungen Eigene Darstellung

Damit ist es möglich geworden, auch über η_0 die mittlere Molmasse $\overline{M}_w$ und den Staudinger-Index [η] zu bestimmen. η_0 wird durch Approximation der Messdaten mit rheologischen Modellgleichungen bestimmt (vgl. Göttfert et

al. 1999). Außerdem gelang es uns, einen Zusammenhang zwischen dem Krümmungsradius (KR) der Viskositätsfunktion (Übergang vom linearviskosen in den strukturviskosen Bereich) und der Molekulargewichtsverteilungsbreite M_w/M_n (Polydispersität) zu finden, die besonders das elastische Verhalten der Schmelzen kennzeichnet (vgl. Göttfert/Reher 1998a) (s. Abbildung 6):

$$KR = \mathrm{A}\, e^{\mathrm{B}(\mathrm{M}_w/\mathrm{M}_n)} \tag{5}$$

In Analogie zur temperatur-zeitinvarianten bzw. molmasseninvarianten Masterkurvenbildung für rheologisch einfache Schmelzen kann nun für rheologisch nicht ähnliche (nicht einfache) Schmelzen, d.h. M_w/M_n = var. ein entsprechendes Verschiebungsgesetz mit a_{KR} gebildet werden:

$$a_{KR} = \frac{KR(\mathrm{M}_w/\mathrm{M}_n)}{KR(\mathrm{M}_w/\mathrm{M}_n)^*} = \exp\left[\mathrm{B}\left(\mathrm{M}_w/\mathrm{M}_n - \mathrm{M}_w/\mathrm{M}_n\big|^*\right)\right]. \tag{6}$$

Wenn als Näherung anstelle von a_{KR} ein charakteristisches Viskositätsverhältnis oder das Verhältnis der Fließindizes eingeführt wird

$$a_{KR} = \frac{\eta}{\eta^*} \text{ bzw. } \quad a_{KR} = \frac{n}{n^*} \text{ bzw. } \quad a_{KR} = \frac{\eta_0}{\eta_0^*}$$

$$\eta_0 = \begin{cases} \mathrm{K}_1 \mathrm{M}_w^{\alpha} & bei\ \mathrm{M} < \mathrm{M}_{Krit} \\ K_2 \mathrm{M}_w^{\beta} & bei\ \mathrm{M} \geq \mathrm{M}_{Krit} \end{cases} \tag{7}$$

erhält man mit Gleichung 7

$$\mathrm{H}\left[\frac{\mathrm{M}_w}{\mathrm{M}_w^*}\right]^{\alpha;\beta} = \exp \quad \mathrm{B}\left[\mathrm{M}_w/\mathrm{M}_n - \mathrm{M}_w/\mathrm{M}_n\big|^*\right]. \tag{8}$$

Die erhaltene Gleichung stellt einen Zusammenhang zwischen der mittleren Molmasse und der Polydispersität (Verteilungsbreite) dar.

Mit diesem Zusammenhang ließen sich die Verteilungsbreiten von verzweigten Polyethylenen und Polypropylenen bestimmen und damit die Qua-

litätssicherung der Produkte realisieren (vgl. Göttfert 1996). Da KR ~ 1/n für das gewählte Fließgesetz ist, vereinfachte sich die Bestimmung und Auswertung der rheologischen Daten ganz entscheidend. Untersuchungen in der Literatur und eigene Messungen bestätigten den signifikanten Zusammenhang $n(M_w/M_n)$ (vgl. Göttfert/Reher 1998b), der in der Software von Kapillar-On-Line-Rheometern zur Verfügung steht. Um eine direkte Bestimmung der viskoelastischen Eigenschaften der Polymeren im On-Line-Rheometer zu ermöglichen, wurde ein dynamisch arbeitendes On-Line-Kapillar-Rheometer (DOR) entwickelt und getestet (vgl. Göttfert et al. 1996). Die dynamische (oszillierende) Führung der Kapillarströmung im DOR ermöglichte trotz überlagerter Offset-Strömung (stationäre Grundströmung), die viskoelastischen Materialfunktionen $G'(\omega)$ und $G''(\omega)$ in einem ausreichend breiten Intervall zu bestimmen. Diese Funktionen korrelieren gut mit den Strukturparametern der Kunststoffschmelzen und sind ebenfalls bestens geeignet zur Qualitätssicherung.

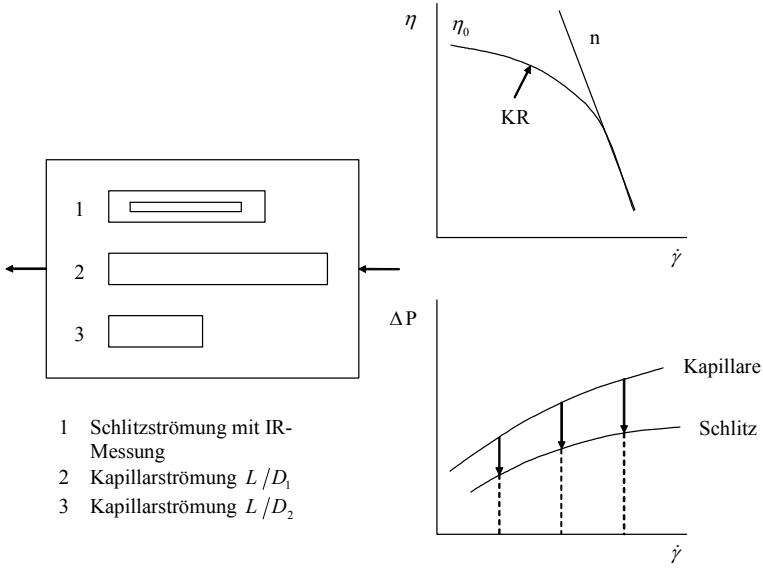
Ergänzend zu den Scherungsprüfverfahren wurde ein On-Line-Dehnungs-Prüfverfahren für Polymerschmelzen entwickelt (vgl. Göttfert/Reher 1998b). Vorzüge dieses On-Line-Messverfahrens sind besonders die hohe Sensibilität auf molekulare Unterschiede der Schmelze (vgl. Göttfert 1998) und die einfache Handhabung des Verfahrens.

Neben der Überwachung der Produkte und Kontrolle des technologischen Prozesses mit den Geräten und Verfahren gibt es auch Anwendungen zur Steuerung des rheologischen Prozesses bei der Polypropylenherstellung und Steuerung der Polydispersität (M_w/M_n) durch Peroxidzudosierung (vgl. Fritz/Stöhrer 1986). Weitere Steuerungskonzepte für andere Polymerherstellungsverfahren mit dem Kapillar-On-Line-Rheometer sind zur Qualitätssicherung der Produkte in Vorbereitung.

Die Anwendung dieser Verfahren und der neuartigen Gerätetechnik zur Qualitätssicherung könnte in allen Technologien erfolgen, in dem der Fluidzustand der Erzeugnisse qualitätsbestimmend ist, so z.B. in der Lebensmittel-, Keramik-, Kosmetik-, Pharmaindustrie, in der Medizintechnik u.v.a. Industriezweigen der Wirtschaft (s. Abbildung 4). Die Daten bestimmen einerseits die Qualität der Erzeugnisse (z.B. bei Schokolade), sind aber auch gleichzeitig Datensätze für die mathematischen Modelle der Verarbeitungs- und Anwendungstechnik (vgl. Hartmann/Reher 2009) der Materialien zu Endprodukten.

Die neueste Entwicklung der On-Line-Überwachung und Produktsicherung in der Kunststofftechnologie ist neben der simultanen Bestimmung des viskoelastischen Verhaltens die Infrarotspektroskopie der Kunststoffschmel-

ze, um Strukturveränderungen zu registrieren und durch Prozessführung Einfluss zu nehmen. Die Gestaltung der On-Line-Technik dazu ist in Abbildung 7 dargestellt. Es ist die maximale Variante des Gerätes dargestellt mit 2 Kapillaren, um z.B. zusätzlich Wandgleiten der Schmelzen zu registrieren, aber auch mit einer Kapillare ist es möglich, das Gerät zu betreiben, um ausreichende Informationen zu gewinnen. Auch in diesem Falle wird zuerst eine Laborvariante mit einem Rotationsviskosimeter entwickelt (vgl. NN 2010), bis eine industrielle On-Line-Variante entwickelt und eingesetzt wird.



$$\Delta P_{Kap}\Big|_{\dot{\gamma}_n} - \Delta P_{Schlitz}\Big|_{\dot{\gamma}_n} = \Delta P_{elast}$$

$$\Delta P_{elast}\left(M_w / M_n\right)$$

Abbildung 7: Rheometer-Block mit IR-Messung
Eigene Darstellung

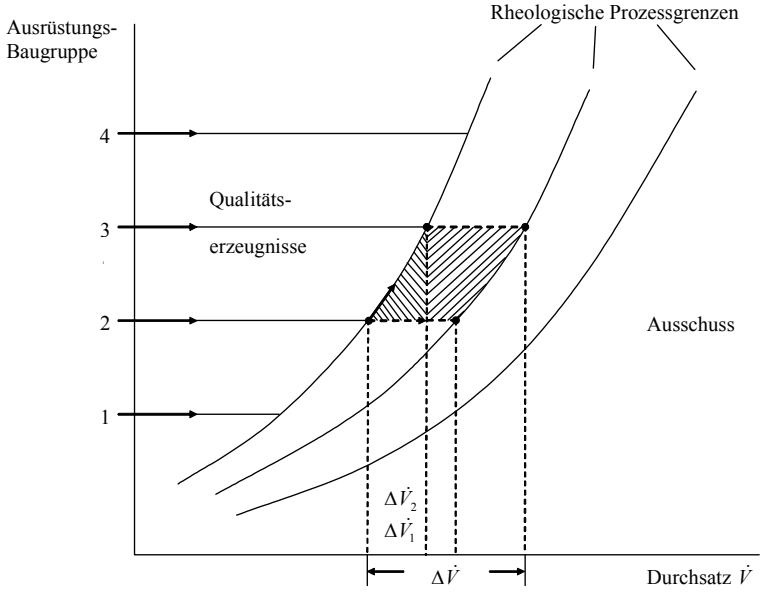
3. Folgen der unbeachteten Qualitätssicherung der Kunststoffe

Bei Nichtsicherung des Verhältnisses der viskosen zu den elastischen Eigenschaften der Kunststoffschmelze, d.h. durch Veränderungen der molekularen

Polymerstruktur ($\overline{M}_w \approx$ const., aber $M_w/M_n =$ var.), kann es zu Störungen der anschließenden Prozessabläufe kommen.

Diese äußern sich in den Verarbeitungsmaschinen in Form von

- Druckschwankungen, Oszillationen,
- Durchsatzabfall, Durchsatzstörungen,
- von Schädigungen des Erzeugnisses (Schmelzebruch, Oberfläche, Struktur, Form, Abmessungen, Funktion, Lebenszeitverkürzung der Bauteile),
- unsachgemäßer Maßstabsübertragungen.



$\Delta\dot{V}_1$ - Änderung der Ausrüstungsbaugruppe (von 2 auf 3)

$\Delta\dot{V}_2$ - Prozessbeeinflussung (Temperatur, Verarbeitungshilfen u.a. Maßnahmen)

$\Delta\dot{V}$ - beide Maßnahmen

Abbildung 8: Arbeitsdiagramm einer Verarbeitungsausrüstung
Eigene Darstellung

Die Anpassung der Folgeprozesse an die neue Schmelzesituation kann nur in einem begrenzten Umfang durch folgende Maßnahmen abgefangen werden:

- Durchsatzherabsetzung bzw. Erniedrigung des Spannungszustandes der Schmelze in der Verarbeitungsmaschine;
- wenn möglich, mäßige Temperaturerhöhung (Grenzen sind thermische

Materialschädigungen – Achtung, Energiedissipation beachten!);
- Einsatz einer anderen Baugröße der Verarbeitungsmaschine (Zusatzkosten);
- Verwendung, wenn möglich, von Verarbeitungshilfen (z.B. Additive) (s. Abbildung 8).

Aus diesen obigen Gründen müssen die Kunststoffverarbeiter von den Kunststoffherstellern konstante Produkteigenschaften abfordern, die diese auch durch entsprechende On-Line-Prozess-Messtechnik sichern können. Aus Kostengründen erhalten die Verarbeiter jedoch nur ein nichtrepräsentatives Qualitätsmerkmal, den Schmelzindex, geliefert, der obige Erscheinungen nicht erfasst. Durch Aufklärung der Verarbeiter in Weiterbildungsseminaren konnten die Chemiekonzerne gezwungen werden, die On-Line-Messtechnik zu erwerben und die Qualitätssicherung zu garantieren.

4. Allgemeine Schlussfolgerungen zur Bereitstellung von Verfahren und Geräten der Produkt-Qualitätssicherung aus Anlagen der Materialtechnologien

Rheologische Kennwerte und Funktionen	Bedeutung für die Anwendung
$\left(MVR \sim \dot{\gamma}_{MVR}\right)_i = f\left(\mathrm{P}_{MVR} \sim \tau_{w,MVR}\right)_i$ $MVR = \dfrac{MFR}{\rho}$	Schmelz-Index-„Fließfunktion“, die über der echten Fließfunktion $\tau_w(\dot{\gamma}_w)$ liegt auf Grund der „viskoelastischen“ Eigenschaften (einlaufdruckunkorrigierte) Fließfunktion. Dient zur Abschätzung des Verarbeitungsverhaltens der Kunststoffschmelze.
$[\eta](\overline{\mathrm{M}}_w)$ $[\eta](\eta_0)$	Staudinger-Index als: Funktionen der mittleren Molmasse; Funktionen der Null-Viskosität. Dient zur Struktur-Eigenschafts-Bestimmung des Kunststoffes.
$\mathrm{K}R(n)(\mathrm{M}_w/\mathrm{M}_n)$	Krümmungsradius der Viskositätsfunktion $\eta(\dot{\gamma})$ am Übergang des linearviskosen zum strukturviskosen Verhalten in Abhängigkeit der Polydispersität der Kunststoffschmelze. Dient der Bewertung des elastischen Verhaltens der Schmelze.

$\eta(\eta_0, \dot{\gamma}, \mathrm{T}, \mathrm{P})$	Viskositätsfunktion in Abhängigkeit von Nullviskosität, Schergeschwindigkeit, Temperatur, Druck. Dient zur Komplettierung der Impulsbilanz zur Bewegungsgleichungsformulierung und Prozessberechnung.
$\mathrm{P}_\mathrm{E}(\dot{\gamma})$ oder $\Delta\mathrm{P}_{elast}(\dot{\gamma})$ $\mathrm{P}_\mathrm{E}(\mathrm{M}_w/\mathrm{M}_n)$ oder $\Delta\mathrm{P}_{elast}(\mathrm{M}_w/\mathrm{M}_n)$	Elastischer Einlaufdruckverlust in Abhängigkeit Schergeschwindigkeit oder Polydispersität. Dient der Bewertung der Schmelzeelastizität bzw. der Verarbeitbarkeit.
$\mathrm{P}_D(\dot{\varepsilon})$	Dehnspannungsfunktion in Abhängigkeit von der Dehndeformationsgeschwindigkeit. Dient zur Festigkeitsbewertung der Kunststoffschmelze.
$G'(\omega)$ $G''(\omega)$ $\tan\varphi = \frac{G''}{G'}$	Speichermodul (Elastizität). Verlustmodul (Viskosität) in Abhängigkeit von der Kreisfrequenz einer dynamischen Belastung. Phasenverschiebung der jeweiligen Erregung. Dienen zur On-Line-Bestimmung viskoelastischer Schmelzeeigenschaften und damit der Verarbeitbarkeit in den Anlagen.
$v_{gl}(\tau_w, \mathrm{T}, \mathrm{P})$	„Wandgleitgeschwindigkeit“ als Funktion der Wandschubspannung der Schmelze und technologischer Parameter (Temperatur, Druck). Dient zur Bestimmung der Randbedingung des mathematischen Prozessmodells.
$\eta_{eff}(t)$, $\dot{\gamma} = const.$ $\mathrm{P}_\mathrm{E}(t)$ u.a. Zeitfunktionen	Viskositäts-Zeitläufe bei diskontinuierlichen Prozessen, z.B. bei der Schokoladenherstellung.

Tabelle 2: Zusammenfassende Darstellung rheologischer Kennwerte und Funktionen, die mit der heutigen Kapillar-On-Line-Rheometrie bestimmt werden können
Eigene Darstellung

1. Materialwissenschaftler ermitteln unter Laborbedingungen Eigenschaftsbilder der Produkte (Struktur-Eigenschaftsbeziehungen); z.B. waren das für Kunststoffe folgende rheologische Funktionen oder Kennwerte: s. Tabelle 2.
2. Ingenieure entwickeln Verfahren und Gerätetechnik zur Bestimmung relevanter Produkteigenschaften unter Prozessbedingungen der Anlage und im Echtzeitbetrieb zur Sicherung der Produktqualität; z.B. Ein- und Mehrkapillaren-Prozessrheometer mit Umlaufstrom zur Sicherung des Echtzeitbetriebes, Dehnrheometer, Spektrometer u.a.
3. Die gewonnenen Informationen mit der Prozessmesstechnik wurden zur Anlagensteuerung benutzt, um qualitätsgesicherte Produkte zu bekommen; z.B. Peroxidzudosierung zur Steuerung der Polypropylenstruktur und damit der viskoelastischen Fluideigenschaften; Temperatursteuerung, Monomerzudosierung, Katalysatordosierung u.v.a.
4. Häufig können die gewonnenen Materialeigenschaften auch für Prozessmodellierungen und -berechnungen angewendet werden; z.B. Komplettierung der Impulsbilanz, Energiebilanz.
5. Die Prozessmesstechnik wird zertifiziert und als Standardmethode zur internationalen Anwendung empfohlen; z.B. Verfahren und Geräte zur Bestimmung des Schmelzindexes.
6. Firmen begründen ihre Existenz auf der Soft- und Hardware-Entwicklung und vertreiben ihre Produkte weltweit, oft als Bestandteil kompletter Produktionsanlagen. Sie betreiben Produktpflege und arbeiten ständig an der hard- und softwaremäßigen Verbesserung, Vervollständigung und Erweiterungen dieser Prozessmesstechnik. Sie halten Ausschau, ob nicht neue Verfahren übernommen werden können aus Forschungen der Materialwissenschaftler (z.B. Spektroskopie); z.B. Göttfert Werkstoff-Prüfmaschinen GmbH.
7. Weitere Nutzungsmöglichkeiten der entwickelten Technik in artverwandten Technologien werden erkundet und durch Modifizierungen für den Einsatz vorbereitet; z.B. Lebensmittelindustrie, Biotechnologie, Keramiktechnologie, Nanotechnologie (s. Abbildung 4).
8. Neue Produkte/Technologien erfordern sehr oft auch neue Prozessmesstechnik-Entwicklungen; z.B. Nanotechnologie, Biotechnologie.
9. Erweiterungen der On-Line-Messtechnik müssen ökonomisch vertretbar sein, sie „müssen sich rechnen“. Was unter Laborbedingungen für Forschung und Entwicklung ökonomisch vertretbar ist, ist für die On-Line-Technik noch lange nicht anwendbar; z.B. Rheologie und IR-Spektroskopie (vgl. NN 2010).

Danksagung: An dieser Stelle möchte ich mich bei Frau Karen Zawatzki und Herrn Daniel Zawatzki für die Realisierung meiner Manuskripte in elektronischer Form bedanken, damit sie veröffentlicht werden konnten.

Symbolverzeichnis

MFR/MVR	Massenschmelzindex/Volumenschmelzindex
$[\eta]$	Staudinger-Index
η	Dynamische Viskosität
η_s	Lösungsmittelviskosität
η_0	Anfangsviskosität
C	Konzentration
$\dot{\gamma}$	Schergeschwindigkeit
M; $\overline{M}_w$	Mittlere Molmasse
t	Mittlere Verweilzeiten
V	Volumina
$\dot{V}$	Durchsätze
T	Temperatur
P	Druck
P_E	Einlaufdruck in die Kapillaren
KR	Krümmungsradius der Viskositätsfunktion $\eta(\dot{\gamma})$
M_w/M_n	Polydispersität oder Molekulargewichtsverteilungsbreite
n	Fließindex des Ostwald-de Waele-Ansatzes
P_D	Dehnspannung
$\dot{\varepsilon}$	Dehngeschwindigkeit
$G'(\omega)$	Speichermodul
$G''(\omega)$	Verlustmodul
ω	Frequenz
v_{gl}	Gleitgeschwindigkeit

Literatur

Fritz, H. G.; Stöhrer, B. (1986): Polymer Compounding Process for Controlled Peroxide-degradation of Polypropylene. In: International Polymer Processing, Vol. 1, No. 1, pp. 31-41

Göttfert, A. (1996): Prozesszeitkonforme, rheologische Charakterisierung von Polymerschmelzen in der Scherung und Dehnung. Dissertation. Halle-Wittenberg (Martin-Luther-Universität)

Göttfert, A. (1998): Praktische Dehnrheometrie von Polymerschmelzen. In: Kunststoffe. Werkstoffe, Verarbeitung, Anwendung, Jg. 88, H. 11, S. 2067-2069

Göttfert, A.; Reher, E.-O. (1998a): Rheologische Prüftechnik von Hochpolymeren: Einsatz im Sinne einer prozessbegleitenden Strukturbestimmung. In: Kautschuk Gummi Kunststoffe, Jg. 42, H. 9, S. 609-615

Göttfert, A.; Reher, E.-O. (1998b): Online Rheology with extended Spectrum. In: ANTEC '98 SPE Technical Papers. Atlanta, GA, U.S.

Göttfert, A.; Reher, E.-O.; Balagula, I. M. (1999): Modelling of Capillary Rheometer Data and Extrapolation of the Viscosity Function into the Linear Viscoelastic Region. In: International Polymer Processing, Vol. 14, No. 1 pp. 57-59 (Special Reprint, Munich)

Göttfert, A.; Reher, E.-O., Erbacher, B.; Nelson, J. (1996): Dynamic Shear Deformation in On-line Capillary Rheometrie. In: ANTEC '96, Conference Proceedings. Indianapolis, IN, U.S., p. 1085

Hartmann, K.; Reher, E.-O. (2009): Mathematische Modelle ? Grundlage für moderne Technologien. In: Banse, G.; Küttler, W.; März, R. (Hg.): Die Mathematik im System der Wissenschaften. Berlin, S. 131-145 (Abhandlungen der Leibniz-Sozietät der Wissenschaften, Bd. 24)

Hepperle, J.; Münstedt, H.; Haug, P. K.; Eisenbach, C. D. (2005): Rheological Properties of Branched Polystyrenes: Linear Viscoelastic Behavior. In: Rheologica Acta, Vol. 45, pp. 151-163

Holzmüller, W.; Altenburg, K. (1961): Physik der Kunststoffe. Berlin

Kulicke, W.-M. (1986): Fließverhalten von Stoffen und Stoffgemischen. Basel u.a.

NN (2010): Thermo Fisher USA: Rheologie und IR-Spektroskopie in einem Rotationsrheometer. In: Kunststoffe. Werkstoffe, Verarbeitung, Anwendung, Nr. 12, S. 78

Reher, E.-O. (2000): Zur Rheologie von Polymerschmelzen. Berlin, S. 5-23 (Sitzungsberichte der Leibniz-Sozietät, Bd. 43)

Reher, E.-O.; Göttfert, A. (2000): Das ε-Verfahren. Firmeninterne Dokumentation der Göttfert Werkstoffprüfmaschinen GmbH Buchen. Buchen

Reher, E.-O.; Göttfert, A.; Sunder, J. (2002): Damit die Qualität stimmt – Rheologische On-Line-Prüftechnik in Prüf- und Produktionsanlagen der Kunststofftechnik. In: Verfahrenstechnik, Jg. 36, Nr. 10, S. 72-74

Universallexikon (1988): Qualität. In: Universallexikon A-Z. Leipzig, S. 597

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 99–109*

Christian Kohlert

Sicherheit gegen Produktfälschung

1. Einleitung

Produktfälschung ist heute kein Kavaliersdelikt mehr, werden doch teure Forschungsaufwendungen nicht in Verkaufsmengen umgesetzt, gehen Nutzeffekte für die Kunden verloren und kommen Arzneimittel mit fehlenden oder minderwertigen Wirkstoffen in Umlauf.

Der Schutz von Produkten gegen Fälschung steht deshalb heute im Mittelpunkt vieler Diskussionen und Entwicklungen. Damit ist sowohl der Schutz eigener Produkte, wie Kreditkarten, elektronischer Erzeugnisse oder Tonträger, als auch der Schutz von Produkten über die eigentliche Verpakkung, wie z.B. wirkungsvolle Pharmaprodukte oder hochwertige Lebensmittelprodukte, zu verstehen.

Nach Aussagen der International AntiCounterfeiting Coalition werden jährlich weltweit Produkte in der Größenordnung von 410 Mrd. Euro gefälscht. Das entspricht 16% des Bruttoinlandsprodukts von Deutschland. Damit werden ungefähr 5% bis 7% der Weltproduktion gefälscht (vgl. IACC 2013).

Nicht die Fälschung an sich, sondern die Gefahr der Einnahme von unwirksamen Pharmaprodukten oder der Verzehr von nicht den Anforderungen genügenden Lebensmitteln lassen dieses Problem zu einem globalen werden.

Zudem verzerren Fälschungen auch die Wettbewerbssituation, wenn in Forschung und Entwicklung investierte Gelder nicht den geplanten Marktdurchbruch erzielen, weil echt wirkende Plagiate die Marktlage verändern. Davon sind besonders hochwertige Pharmaprodukte und Konsumgüter betroffen, welche auf dem Markt als für den Normalverbraucher nicht unterscheidbare Plagiate auftauchen.

Der Markt fordert deshalb zu Recht einen Fälschungsschutz, der sich durch einfache Einbringung in das Produkt oder die Verpackung sowie leichte und eindeutige Wiedererkennung der Originalität des Produktes auszeichnet.

Klöckner Pentaplast als der führende Hersteller von innovativen Hartfolien für Verpackungszwecke und technische Anwendungen beschäftigt sich seit mehreren Jahren mit der Aufgabe, Verpackungsfolien so zu kennzeichnen, dass sie wiedererkennbar für den Folienhersteller und nutzbar als Produktschutz für den Verarbeiter werden. Dazu wurden herkömmliche Systeme auf ihre Anwendbarkeit geprüft, eigene Ideen entwickelt und großtechnisch umgesetzt.

Herkömmliche Methoden wie:

- Buchstaben-Zahlen-Kombinationen mit Validierung über IT
  – Serialisierung über elektronische Identifikationssysteme
  – 2- und 3-dimensionale Barcodes
- spezielle Prägungen/Bedruckungen auf Verpackungen
  – Strukturen auf Walzen
  – unsichtbare Tinten (435 Mio Farbcodes möglich)
  – metamerische Farben (nur über Filter unterscheidbar)
  – UV- oder IR-Farben (nur mit spezieller Kamera erkennbar)
  – reaktive Farben (reagieren auf Lösemittel oder Metall)
- molekulare Markierungssysteme
  – DNS (schwer fälschbar, sehr teuer)
  – biotechnische Marker (Erkennung aufwendig)
- magnetische Markierungssysteme
  – elektromagnetische Glasfasern (Orientierung)
  – MagDot (magnetischer Punkt unter Druckbild)
- Mikro- oder Nanopartikel (Tagents)
  – durch chemische Modifizierung mit spezifischen Eigenschaften
  – UV/IR-Nanopartikel mit Sichtbarmachungstechnik
- Hardware/DSoftwareschutz (Dongle)
- Hologramme
- Funkchips (RFID)

sind teilweise nur aufwendig anwendbar und ebenfalls nicht einhundertprozentig fälschungssicher.

Als fälschungssicher kann eigentlich nur eine Methode angesehen werden, die auf dem Kriterium Zufall beruht.

Zufällig erzeugte Strukturen können mit der gleichen Methode nicht nachgemacht werden, dann wäre es kein Zufall. Wenn man also eine Methode findet, die zufällig Verteilungen erzeugt und man das genutzte Kriterium ebenfalls definieren und wiedererkennen kann, kann man von einem echten Schutz reden, der auch nicht mit größtem Aufwand nachmachbar ist.

2. Fälschungssicherheit für kp-Folien

Klöckner Pentaplast orientiert sich bei der Sicherung seiner Folien zukünftig auf das Einbringen fluoreszierender Pigmente im IR- oder UV-Anregungsbereich. Dabei werden diese Pigmente über die Rezeptur oder nachträglich durch Lackierung in bzw. auf die Fläche der Folie aufgebracht.

In Konzentrationen < 1% sind diese Pigmente mit einem herkömmlichen Laser im Anregungswellenbereich auffindbar, da sie im sichtbaren Licht zurückstrahlen (s. Abbildungen 1 und 2).

Abbildung 1: Laserangeregtes Luminophor in Verpackungsfolie[1]

1 Alle Abbildungen sind Eigentum der Klöckner Pentaplast GmbH & Co.KG.

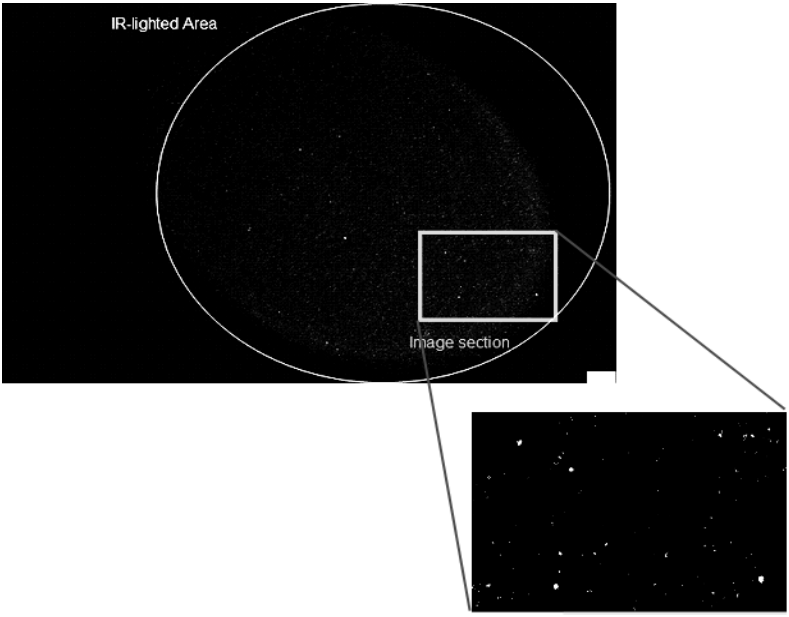
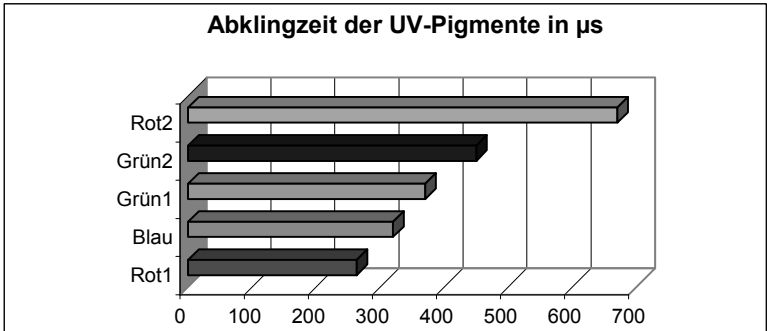


Abbildung 2: Belichtung einer Fläche von 10 cm² mit einem aufgeweiteten Laserstrahl

Damit gibt es nur die Aussage, dass in der Folie bestimmte Pigmente für eine Wiedererkennbarkeit enthalten sind.



	Rot1	Blau	Grün1	Grün2	Rot2
Abklingzeit in µs	263	320	370	450	670

Abbildung 3: Abklingverhalten verschiedener UV-Pigmente

Mit einer speziellen Messtechnik kann das Abklingverhalten dieser Pigmente (s. Abbildung 3) definiert und bei Überprüfung zur Echtheitsbestimmung genutzt werden (s. Abbildung 4).

Abbildung 4: Messgerät zur Bestimmung der Abklingkurve aktivierter Pigmente (vgl. IMC Systemtechnik 2013)

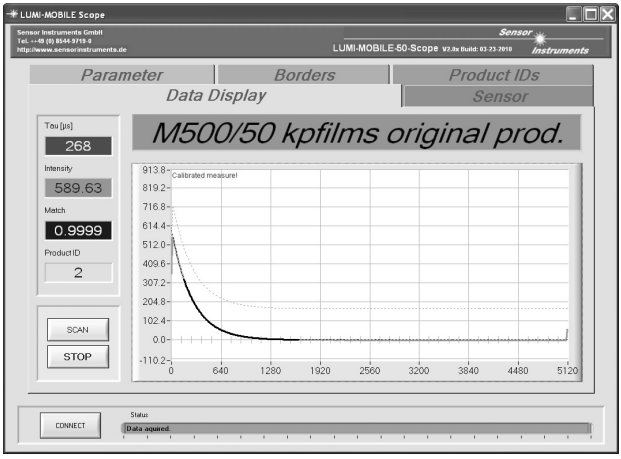


Abbildung 5: Abklingkurve aktivierter Pigmente (vgl. IMC Systemtechnik 2013)

Jedes Pigment strahlt und klingt mit einer speziellen Abklingkurve aus, welche durch die Konzentration C_0 und die Abklingzeit Tau (τ) definiert ist (s. Abbildung 5).

Bei möglichem Exklusivrecht seitens der Pigmenthersteller kann die Erkennbarkeit eigener Folien damit schon recht gut definiert werden. Der Tau-Wert definiert das genutzte Pigment, die C_0 Konzentration die eingebrachte Menge.

Bei Reduzierung der Pigmentkonzentration können diese Kurven derzeit noch bis zu 0,01% sicher aufgenommen werden. Damit beträgt der Pigmentpreis rund 0,1 C/kg Folie.

3. Fälschungssicherheit für Verpackungen

Klöckner Pentaplast will zusätzlich zu dieser Wiedererkennungsmöglichkeit für kp-Folien dem Kunden eine Möglichkeit geben, seine Produkte mit Hilfe eines Fingerabdruckes preiswert und unkompliziert zu schützen.

Dazu wurde folgende Methode festgelegt (vgl. Kohlert et al. 2010): Mittels Rezeptur werden die gewünschten Pigmente zufällig in der Folie verteilt, wobei auf einen Quadratzentimeter ein bis fünf Pigmente kommen. Durch geeignete Lichtgestaltung über UV-Lampen, IR-Laser oder IR-LED werden die Pigmente angeregt und über sichtbares Licht erkennbar gemacht (s. Abbildung 6).

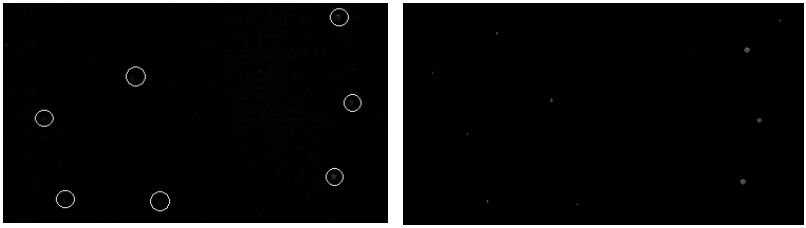


Abbildung 6: Pigmentierte Folie unter Anregungslicht

Bei dieser Anforderung genügt eine mittlere Pigmentkonzentration von kleiner als 0,001% = 10 ppm.

Die Pigmente liegen in einer Größenordnung von einigen µm vor, so dass sie mit dem bloßen Auge nicht erkennbar sind. Sie sind absolut zufällig in der Folie verteilt (s. Abbildung 7).

Durch geeignete Kameras sowie entsprechender Lichttechnik werden diese Bilder aufgenommen und zur weiteren Auswertung zur Verfügung gestellt (s. Abbildung 8).

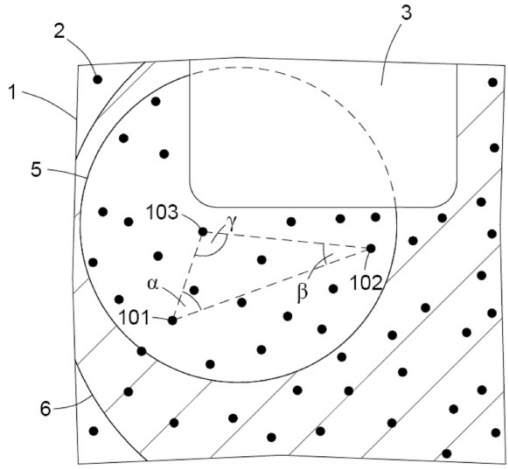


Abbildung 7: Pigmentverteilung in einer Folie (vgl. Kohlert et al. 2010)

Die Idee hierbei liegt in der absolut zufälligen Verteilung der Pigmente und der anschließenden geometrischen Zuordnung zueinander.

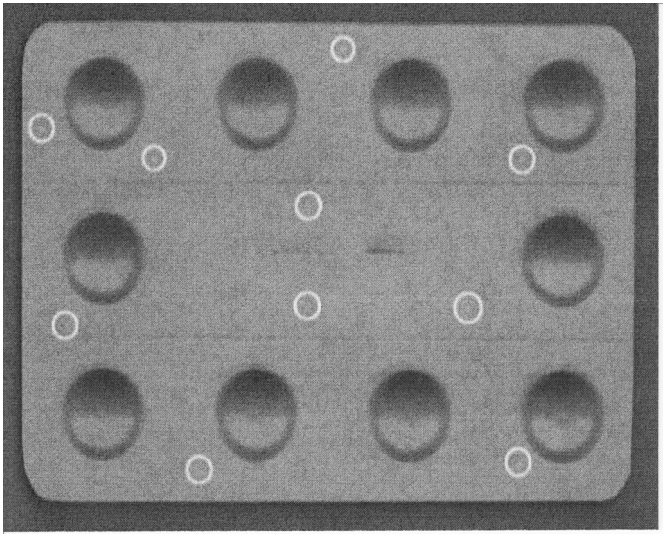


Abbildung 8: Pigmentierte und sichtbar gemachte Verpackungsfolie (Blister) mit vordefinierten Punkten

Jeweils drei Pigmente stellen immer ein Dreieck dar mit den Winkeln Alpha, Beta und Gamma, wobei Gamma sich aus 180 minus Alpha minus Beta berechnet. Im Falle eine Linie würde ein Winkel mit unendlich bzw. 0 herauskommen. Die dargestellten Winkel verändern sich nicht mit Abstand der aufnehmenden Kamera, es muss lediglich eine 90-Grad-Aufnahme garantiert werden, um keine Verzerrungen zuzulassen.

Ebenfalls möglich wäre die Bestimmung des Kreisdurchmessers, welcher alle drei Punkte durchschneidet. Dies wäre aber auch nur abstandskonstant nutzbar.

Am Beispiel einer Pharmaverpackung, einer Kreditkarte oder einfach eines Labels könnte man sich die weitere Vorgehensweise wie folgt vorstellen:

Eine spezielle Software definiert die Winkel Alpha und Beta und speichert diese ab. Im Falle einer Nutzung von vier Punkten ergäbe das vier Dreiecke, bei fünf Punkten zehn Dreiecke und bei sechs Punkten 20 Dreiecke. So kann die Genauigkeit erhöht werden, jedoch auf Kosten der notwendigen Speichermenge des Computers und der Auswertgeschwindigkeit (s. Abbildung 9).

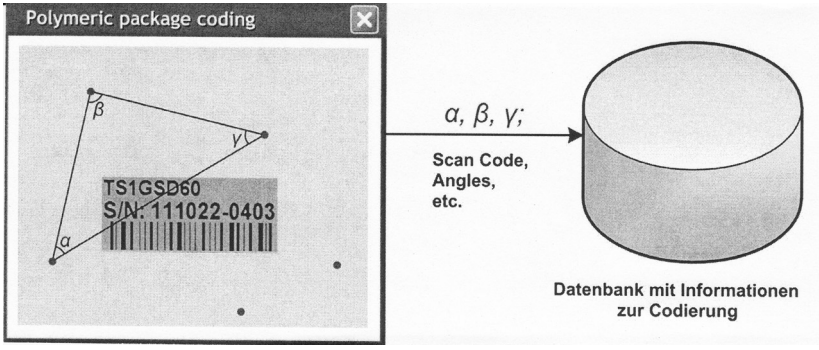
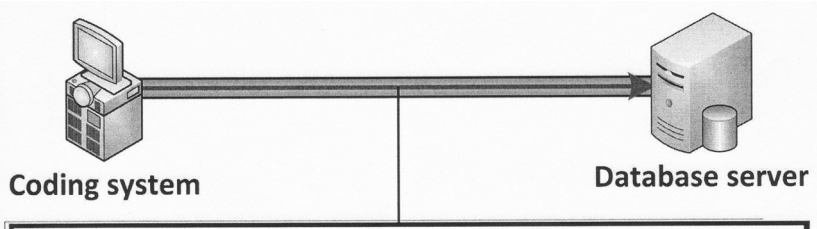


Abbildung 9: Dreiecksbeziehungen einer pigmentierten Verpackung

In einer nachfolgenden Auswertung werden die Winkel der vier gewählten Dreiecke abgespeichert und in diesem Falle der Kreditkartennummer zugeordnet (s. Abbildung 10).

Im Falle der Nutzung einer gefälschten Verpackung/Kreditkarte sowie der ausgespähten PIN-Nummer würde eine spezielle Hardware im Kartenlesegerät (s. Abbildung 11) die sichtbar gemachten Pigmente aufnehmen und an den Datenserver zur Auswertung weiterleiten (s. Abbildung 12 und 13).



Identification data											
Card num			4000 0012 3456 7899								
Triangle 1			Triangle 2			Triangle 3			Triangle 4		
α_1	β_1	γ_1	α_2	β_2	γ_2	α_3	β_3	γ_3	α_4	β_4	γ_4
7	13	160	26	68	94	32	48	100	33	35	112
Valid thru			12.2012								
Type			Verpackung/ Kreditkarte								

Abbildung 10: Codierung einer pigmentierten Verpackung oder Kreditkarte

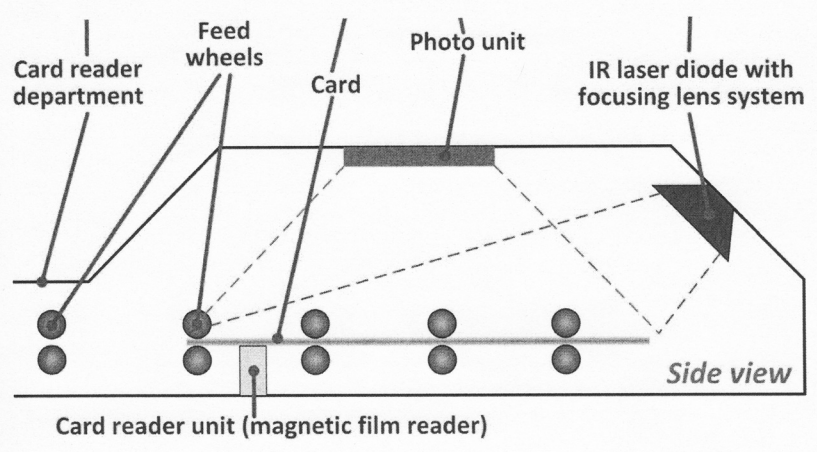


Abbildung 11: Beispielhafte Kontrolle der Karte im Kartenlesegerät

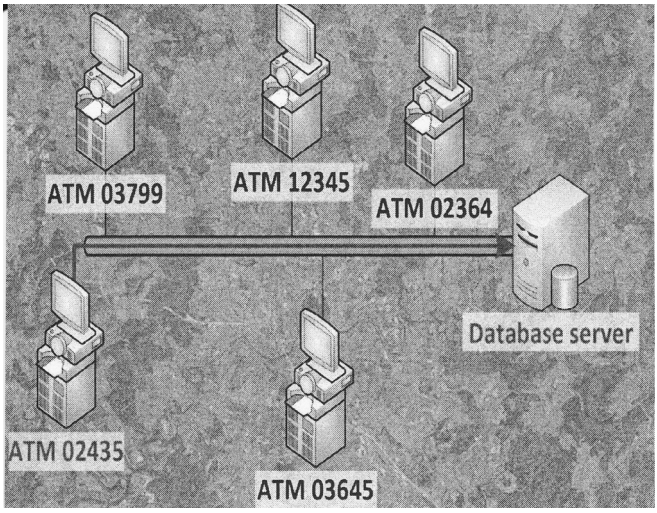


Abbildung 12: Übertragung der Pigmentlage an den Auswertserver

	Identification data for card # 4000 0012 3456 7899											
	Triangle 1			Triangle 2			Triangle 3			Triangle 4		
	α_1	β_1	γ_1	α_2	β_2	γ_2	α_3	β_3	γ_3	α_4	β_4	γ_4
	7	**13**	**160**	**26**	**68**	**94**	**32**	**48**	**100**	**33**	**35**	**112**

	Data from card, being identified											
	Triangle 1			Triangle 2			Triangle 3			Triangle 4		
	α_1	β_1	γ_1	α_2	β_2	γ_2	α_3	β_3	γ_3	α_4	β_4	γ_4
Combination 1	**15**	**42**	**123**	**34**	**36**	**110**	**39**	**61**	**80**	**51**	**58**	**71**
Combination 2	**13**	**15**	**152**	**30**	**67**	**83**	**34**	**58**	**88**	**39**	**64**	**77**
...												
Combination N_C	**12**	**30**	**138**	**20**	**53**	**107**	**32**	**33**	**115**	**45**	**53**	**82**

Abbildung 13: Auswertung der Pigmentverteilung auf der Kreditkarte

Im Falle des Nichtvorhandenseins von Pigmenten oder der fehlenden Dreieckszuordnung könnte die gefälschte Karte einbehalten und der Nutzer leicht ermittelt werden.

Derzeit werden für die Erkennung einer solch gesicherten Kreditkarte fünf bis zehn Sekunden in Abhängigkeit von der Pigmentanzahl benötigt.

Die Aufwendungen für dieses System sind sehr gering wegen der niedrigen Konzentration der genutzten Pigmente und der handelsüblichen Auswertgeräte (Leuchten, Kamera). Die Speichermenge für einen Datensatz beträgt gerade mal 50 Byte. Die Mehrkosten für eine solch dotierte Folie betragen weniger als 0,01 Ct/kg Folie, die Aufnahmetechnik für 1 cm² kostet rund 500 €/Stück.

Denkbar wäre auch, eine Label-Folie für Etiketten anzubieten, wo der Endproduzent das aufgeklebte Label abfotografiert, abspeichert und mit dieser Methodik nach Nutzung jederzeit die Echtheit oder Fälschung feststellen kann.

Diese von Klöckner Pentaplast patentierte Technologie wird allen ihren Kunden und Nutzern von Hartfolien angeboten zur Sicherung ihrer wertvollen Produkte mit einem Fingerabdruck, der durch die zufällig verteilten und sichtbar gemachten Pigmente in der Verpackung realisiert werden kann.

Literatur

IACC – International AntiCounterfeiting Coalition. – URL: www.iacc.org [27.04.2013]

IMC Systemtechnik. – URL: http://www.imc-systemtechnik.de [27.04.2013]

Kohlert, Chr.; Schmidt, J.; Egenolf, D.; Zistjakova, T. (2010): Verpackungsfolie für Produktauthentifizierung, Authentifizierungsverfahren und -system. Patent DE 10 2008 032 781 A1 und WO 2010/003585 A1

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 111–122*

Dietrich Balzer

Die gegenwärtige und zukünftige Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft

1. Einleitung

Der Wirtschaftszweig „Sicherheit“ wird in der Wirtschaftsstatistik noch nicht ausgewiesen. National und international hat sich aber schon eine Sicherheitswirtschaft etabliert.

Wissenschaftliche Untersuchungen und Studien beweisen das. Auf Grund der spezifischen Eigenschaften der Automatisierungs- und Kommunikationstechnik spielt diese Technik in der Sicherheitswirtschaft eine zentrale Rolle, die auf der Einheit von Informationsgewinnung, Informationsverarbeitung und Informationsnutzung basiert.

Innerhalb der Sicherheitswirtschaft wird die Automatisierungs- und Kommunikationstechnik vor allem in folgenden Marktsegmenten eingesetzt:

- Sicherheitstechnik (Biometrie, Videotechnik, Sensorik, Leittechnik, Zutrittskontrolle);
- IT-Sicherheit (Netzsicherheit, Verschlüsselung, Virtual Private Network, Public Key Infrastructure, Smart Card);
- Sicherheitsdienstleistungen (Objekt- und Wachschutz, Risk Management, Trust Center, Sicherheits-Audits, Sicherheits-Engineering, Consulting).

Die Automatisierungs- und Kommunikationstechnik als sicherheitsorientierte Wissenschaftsdisziplin stellt für alle diese Marktsegmente Methoden und Produkte zur Verfügung, die auf die Kompensation nicht ausregelbarer Störgrößen orientieren. Dabei geht es vor allem um Lösungen der Prozessüberwachung sowie der vorbeugenden und elementaren Prozesssicherung.

Im vorliegenden Beitrag werden Probleme der Forschung und Lehre beim Einsatz der Automatisierungs- und Kommunikationstechnik für die Sicherheit von technologischen Prozessen in komprimierter Form dargestellt. Die Leibniz-Sozietät der Wissenschaften zu Berlin kann dabei besonders in Kooperation mit mittelständischen Unternehmen der Region Berlin/Brandenburg bei der Aus- und Weiterbildung sowie bei der Lösung wissenschaftlich-technischer Probleme konkrete Beiträge leisten.

2. Definitionen

Bevor die Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft dargestellt wird, sollen die Begriffe Sicherheit, Gefahr und Risiko definiert werden:

- Gefahr ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist.
- Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes (qualitativ oder durch sicherheitstechnische Festlegungen bestimmbar).
- Risiko ist eine Wahrscheinlichkeitsaussage bezogen auf einen technischen Vorgang oder Zustand. Dabei werden die Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß bewertet.
- Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.

3. Der Sicherheitsmarkt in Deutschland

Aus den vorliegenden Studien bzw. Analysen sollen zwei charakteristische Beispiele ausgewählt werden.

Durch den Bundesverband für Sicherheitswirtschaft (BDSW) wurde der Sicherheitsmarkt in Deutschland analysiert (s. Abbildung 1).

Dabei wurde im Wesentlichen der klassische Markt der Sicherheitstechnik betrachtet. Probleme der vorbeugenden Sicherung sind nicht analysiert worden. Aus eigener Erfahrung kann eingeschätzt werden, dass der Markt für softwarebasierte Lösungen der vorbeugenden Prozess- und Produktsicherung ca. 5 Mrd. € umfasst, sodass der gesamte Sicherheitsmarkt in Deutschland ungefähr 16 Mrd. € umfasst.

Das zweite Beispiel betrifft eine Analyse der Sicherheitswirtschaft in Berlin und Brandenburg, die von der Landesregierung in Brandenburg und dem Senat von Berlin durchgeführt wurde (vgl. Berlin Partner GmbH 2012). Die Ergebnisse können wie folgt zusammengefasst werden:

- 220 Unternehmen der Sicherheitswirtschaft wurden befragt.
- Der Umsatz aller befragten Unternehmen beträgt 2,43 Mrd. Euro pro Jahr, die Beschäftigtenzahl beträgt 24.500.
- Mehr als 50% der Unternehmen orientieren sich auf den überregionalen Markt.
- Wichtigster Zielkunde ist die Industrie, gefolgt von der öffentlichen Hand und den Betreibern von Infrastrukturen.

- 73% der Unternehmen sind an F&E-Kooperation interessiert.
- 48% haben Bedarf an akademischer Weiterbildung.

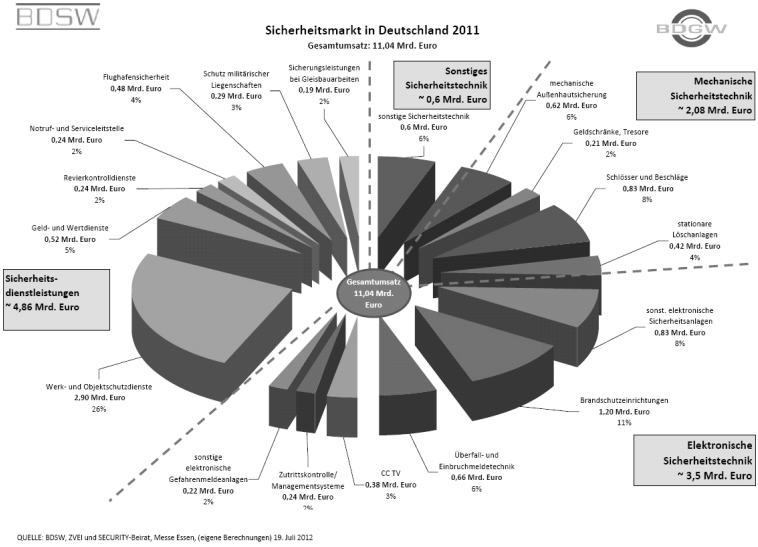


Abbildung 1: Analyse des BDSW
Quelle: BDSW 2012, S. 29

Wichtig sind vor allem die Aussagen, dass ein großer Bedarf an modernen wissenschaftlich-technischen Lösungen besteht und dass eine akademische Aus- und Weiterbildung sowohl als Vertiefungsrichtung in vorhandenen Master- und Bachelor Studiengängen als auch als selbstständige Studiengänge gewünscht wird. Außerdem zeigt die Analyse, dass die Region Berlin/Brandenburg auf dem Gebiet der Sicherheitswirtschaft eine führende Stellung in Deutschland einnimmt.

4. Algorithmen der zentralen Sicherung dezentraler Anlagen

Bevor wir auf die Algorithmen der automatischen Steuerung eingehen, soll auf folgende Vor- und Nachteile der Automatisierungs- und Kommunikationstechnik hingewiesen werden:

- Vorteile: Einheit von Informationsgewinnung (ständige standortunabhängige Prozess- und Produktüberwachung), Informationsverarbeitung (Si-

tuationserkennung, Prognose) und Informationsnutzung(Vor-Ort- und Fernsteuerung).
- Nachteile: zusätzliche Risiken durch Stabilitäts- und Sensibilitätsprobleme sowie durch Security-Probleme.

Es ist also notwendig, einen optimalen Kompromiss zwischen den Vorteilen und den Nachteilen zu erreichen.

Durch eine vergleichende Analyse der Amplitude und der Frequenz der auf das System einwirkenden Störgrößen können die Bereiche der verschiedenen Automatisierungsfunktionen und damit auch der Bereich der Prozesssicherung bestimmt werden. Abbildung 2 zeigt, wie diese Bereiche bestimmt werden können.

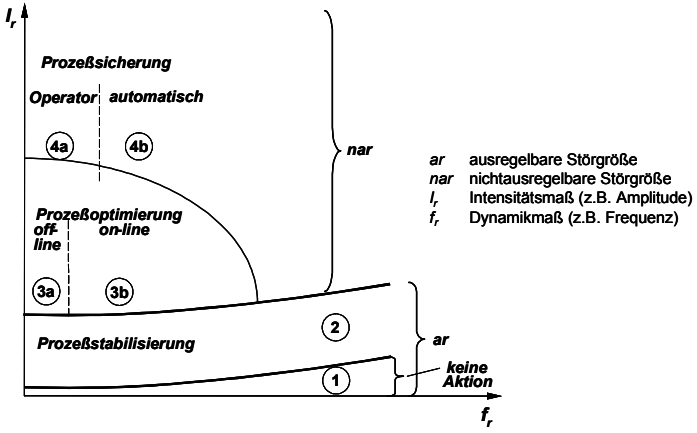


Abbildung 2: Zusammenhang zwischen Störgrößeneigenschaften und Automatisierungsfunktion Eigene Darstellung

Für die Festlegung der Struktur der Steuerungsalgorithmen wird ein so genanntes „Informationsmodell Sicherheit“ bestimmt, das Aussagen zu folgenden Prozesseigenschaften beinhaltet:
- Festlegung der Eigenschaftsprofile der Prozesselemente (Gutbereich, zulässiger Fehlbereich, unzulässiger Fehlbereich);
- dynamische Zustandsvariable (Druck, Temperatur, ...);
- stationäre Prozessparameter (Wärmedurchgangszahl, Katalysatoraktivität, ...);
- Steuergrößen (Motoransteuerung, Sollwertänderung, ...);
- Störgrößen (Umweltbedingungen, Rohstoffeigenschaften, ...).

Am Beispiel einer Ammoniak-Synthese-Anlage ist in Abbildung 3 ein konkretes Informationsmodell dargestellt.

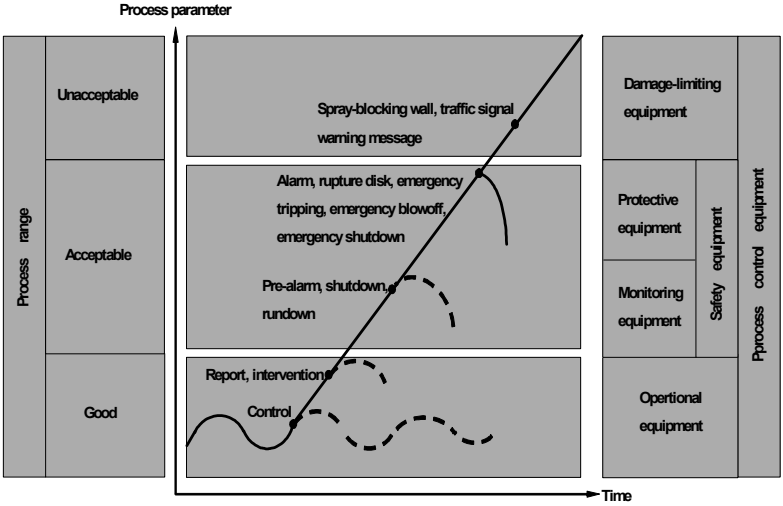


Abbildung 3: Elementary and Preventing Processsecuring of Ammonia plant
Quelle: VAN 2010b, S. 15

Die Erfahrungen auf dem Gebiet der Prozesssicherung zeigen, dass unter Nutzung des oben genannten Informationsmodells die Ljapunovsche Stabilitätstheorie eine gute Grundlage für den Entwurf der Steuerungsalgorithmen darstellt. Im Weiteren soll die Anwendung dieser Theorie erläutert werden.

Der Prozesssicherungsalgorithmus besteht aus folgenden zwei Hierarchieebenen:

- Erkennen gefährlicher Situationen;
- automatische Realisierung einer Abwehrstrategie.

Folgende Abwehrstrategien sind möglich:

- Aktivierung kalter oder heißer Redundanzen;
- Lastabwurf;
- Steuerung der Hauptprozesse auf Teil- oder Nullproduktion;
- sofortiges Abfahren der Anlage bei besonderer Gefahr für Menschen und Ausrüstungen (Grenzrisiko).

Ein gefährlicher Zustand (GZ) bzw. eine gefährliche Situation liegt dann vor, wenn eine oder mehrere Komponenten des Vektors der Zustandsgrößen q

oder des Vektors der Störgrößen x bestimmte obere Grenzwerte (q_i^o, x_k^o) überschreiten bzw. bestimmte untere Grenzwerte (q_j^u, x_e^u) unterschreiten:

$$GZ := q_i \geqq q_i^o V q_j \leqq q_j^u V x_k > x_k^o V x_e \leqq x_e^u \,. \tag{1}$$

Bei Erfüllung der Gleichung (1) handelt es sich um die Verletzung bestimmter technologischer bzw. apparatetechnischer Begrenzungen (z.B. Verletzung einer Grenztemperatur, eines Grenzdruckes oder einer kritischen Konzentration).

Bei der Synthese des Sicherungsalgorithmus gehen wir von folgendem mathematischen Modell des gesteuerten Systems aus:

$$\frac{dx}{dt} = f(x). \tag{2}$$

Die Ljapunov-Funktion zur Bestimmung von sicheren Einzugsbereichen hat folgendes Aussehen:

$$l(x) = const > 0 \,. \tag{3}$$

Die Änderungsgeschwindigkeit der Ljapunov-Funktion ist:

$$\frac{dl(x)}{dt} = p(x). \tag{4}$$

Unter Berücksichtigung von (2) haben wir:

$$\frac{dl(x)}{dt} = \frac{\partial l}{\partial x} \cdot \frac{dx}{dt} = \frac{\partial l(x)}{\partial x} \cdot f(x). \tag{5}$$

Die Bestimmung sicherer Einzugsbereiche erfolgt nun unter Verwendung der Gleichungen (2) bis (5). Abbildung 4 zeigt die prinzipielle Vorgehensweise bei der Bestimmung dieser Einzugsbereiche.

Um die Bestimmung des Einzugsbereiches zu vereinfachen, wurde die Ljapunov-Funktion in Form eines Kreises definiert. Dadurch nutzen wir nicht alle Möglichkeiten der Prozesssicherung. Andere kompliziertere Funktionen sind auch möglich und wurden auch erprobt. Dabei sind allerdings genauere mathematische Modelle des gesteuerten Systems notwendig, was zweifellos zu höheren Kosten führt.

Durch die Überführung des technologischen Systems in den sicheren Einzugsbereich wird die Prozesssicherungsaufgabe algorithmisch gelöst.

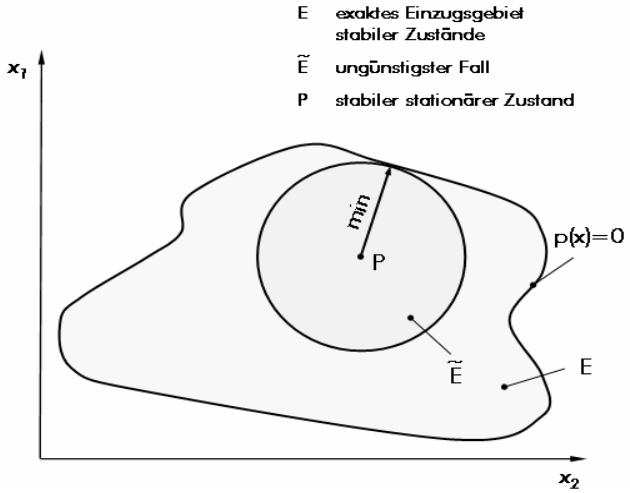


Abbildung 4: Bestimmung sicherer Einzugsbereiche
Eigene Darstellung

Die oben beschriebene Vorgehensweise wird nun auf ein komplexes System übertragen, das aus mehreren Teilsystemen besteht (s. Abbildung 5).

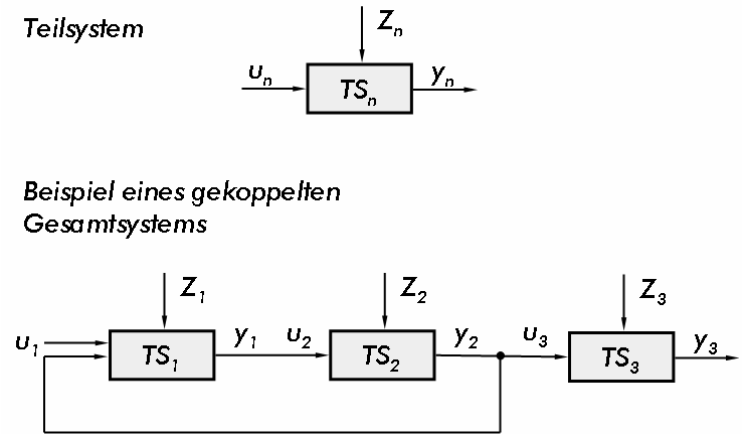


Abbildung 5: Struktur des Sicherungsobjektes
Eigene Darstellung

Die Aufgabe des Prozesssicherungssystems für das in Abbildung 4 dargestellte System besteht in der Überführung der Prozessparameter in ein Gebiet, aus dem sie in einem begrenzten Zeitbereich durch Anwendung der Abwehrstrategie keine gefährlichen Zustände erreichen (Quasistabilität).

Wir gehen vom ungünstigsten Fall aus, nämlich vom Maximum von $\frac{dl(x)}{dt} = p$:

$$p(x) = \sum_{n=1}^{N} p_n(x_n) \rightarrow \max . \tag{6}$$

Dabei ist die folgende Nebenbedingung einzuhalten:

$$1(x) = \sum_{n=1}^{N} 1_n(x_n) = const . \tag{7}$$

Darüber hinaus muss die folgende Koppelbedingung berücksichtigt werden:

$$G(x) = \sum_{n=1}^{N} g_n(x_n) = 0 . \tag{8}$$

5. Automatisierte Security-Lösungen

Wie bereits im Abschnitt 4 erwähnt, kommt es beim Einsatz moderner Automatisierungs- und Kommunikationstechnik darauf an, die Security-Probleme zu lösen.

Dabei kommet es darauf an, folgende Anforderungsprofile zu erfüllen:

- *Vertraulichkeit* (Confidentiality): Schutz vor unautorisierten Lesezugriffen, Kopieren, falschen Empfängern;
- *Integrität* (Integrity): Verhinderung unautorisierter Schreibzugriffe bzw. Datenmanipulation;
- *Authentizität* (Authentication): Glaubwürdigkeit eines Benutzers (Mensch, Kommunikationsgerät, Programm);
- *Zugriffskontrolle* (Authorisation): zugelassene Personen bzw. Dienste;
- *Nichtbestreitbarkeit* (Non-Repudiability): Verbindlichkeit, Empfangsbestätigung (erfolgt oder nicht erfolgt);
- *Verfügbarkeit* (Availability): keine Verhinderung berechtigter Zugriffe;
- *Aufzeichenbarkeit* (Auditability): Log-Files (Protokolldateien).

Es sind folgende zusätzliche Security-Lösungen für die zentrale Steuerung dezentraler Anlagen erforderlich:

- Entwurf automatisierungsspezifischer sicherer Netzwerktopologien für heterogene Netzwerke;
- funktionale Dekomposition und Skalierbarkeit von Securityfunktionen unter Beachtung der Echtzeitanforderungen;
- Schaffung von Konfigurations- und Administrationshilfen für heterogene Netzwerke bezüglich Security:
- modellbasierter Zugriffsschutz durch Prüfung der Authentizität und Nichtbestreitbarkeit der übertragenen Prozessinformationen;
- Personifizierung der Authentisierung sowie Willensbekundung mittels Integration von biometrischen Merkmalen (Fingerabdrücke und dynamische Unterschriften).

Um die oben genannten Anforderungen zuverlässig zu erfüllen, ist die Einrichtung von folgenden Schutzzonen (Security Integration Zones – SIZ) notwendig (vgl. VAN 2010b):

- SIZ 1 (hoher Schutz) für die prozessnahen Funktionen: Messen, Regeln, Steuern, elementare Prozesssicherung; on-line-closed loop;
- SIZ 2 (mittlerer Schutz) für die prozessfernen Funktionen: Bedienen, Beobachten, vorbeugende Prozesssicherung, Anlagenkoordinierung zur Kopplung mehrerer Firmenstandorte, Engineering, on-line open loop;
- SIZ 3 (geringer Schutz) für die Funktionen des Unternehmensmanagements: Wartung und Instandhaltung, Training der Operatoren und der Service-Ingenieure.

6. Beispiele realisierter Prozesssicherungssysteme

Die in den vorangegangenen Abschnitten dargestellten theoretischen Ergebnisse der automatischen vorbeugenden modellgestützten Prozesssicherung wurden an mehreren Beispielen praktisch erprobt. Die Abbildung 3 zeigt eine Anwendung für die Ammoniak-Synthese.

In Abbildung 6 ist die Struktur des zentralen Prozesssicherungssystems für dezentrale Biogasanlagen dargestellt.

Diese Anwendung besitzt ein zentrales Operatorzentrum mit den Funktionen: Bedienen, Beobachten, Trainieren, Visualisieren, vorbeugende Prozesssicherung. Das Operatorzentrum besitzt sowohl eine stationäre als auch eine mobile Komponente.

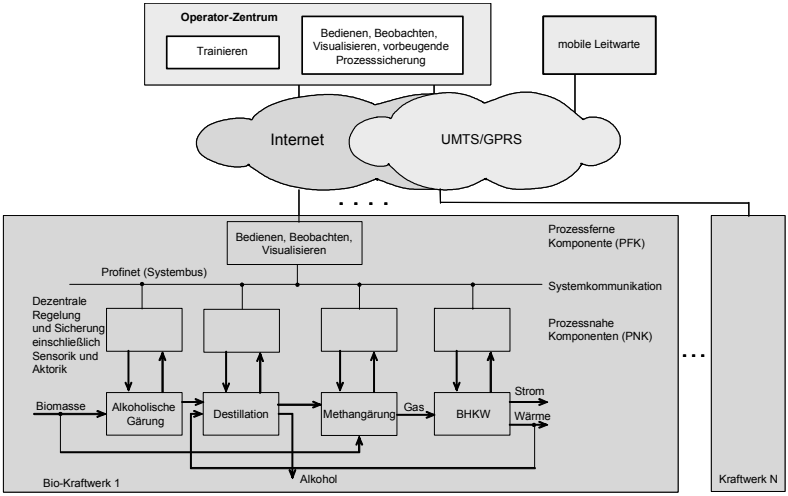


Abbildung 6: Struktur des zentralen Prozesssicherungssystems für Biogasanlagen
Eigene Darstellung

Abbildung 7 zeigt ein Prozesssicherungssystem für ein diskret-kontinuierliches technologisches System einer Papierproduktion (vgl. IPK 2005).

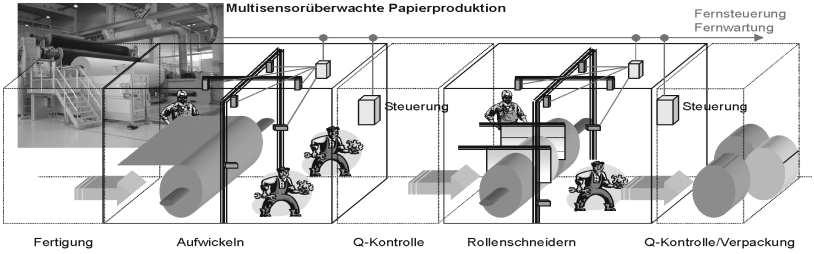


Abbildung 7: Multisensorüberwachte Produktion, Systemübersicht
Quelle: IPK 2005

Die Aufgaben und Eigenschaften dieses Prozesssicherungssystems sind:

- mehrdimensionale visuelle Erfassung;
- automatische Klassifikation;
- Erkennungsrobustheit bei wechselnden Umgebungsbedingungen;
- selektive Bewegungsanalyse;

- schnelle Algorithmen sowie optimierte, zuverlässige Kommunikation;
- Erfassung und Modellierung des Arbeits-/Gefahrenraums.

7. Akademische Lehre und Weiterbildung

In der Region Berlin/Brandenburg existieren bereits auf folgenden Gebieten Aus- und Weiterbildungsangebote:
- Sichere Identität;
- Sichere Infrastruktur;
- IT-Sicherheit/Sicherheit mit IT;
- Sicherheit und Gesellschaft;
- Urban Security.

Folgende Universitäten und Hochschulen bieten auf diesen Gebieten Lehrveranstaltungen an:
- Beuth Hochschule für Technik Berlin;
- Brandenburgische Technische Universität Cottbus (BTU);
- Charité – Universitätsmedizin Berlin;
- Deutsche Universität für Weiterbildung Berlin;
- Europa-Universität Viadrina Frankfurt (Oder);
- Fachhochschule Brandenburg (FH Brandenburg);
- Fachhochschule der Polizei des Landes Brandenburg;
- Freie Universität Berlin (FU Berlin);
- Hochschule Lausitz (FH Lausitz);
- Hochschule für Technik und Wirtschaft Berlin (HTW);
- Hochschule für Wirtschaft und Recht Berlin (HWR);
- Humboldt-Universität zu Berlin (HU Berlin);
- Steinbeis-Hochschule Berlin GmbH;
- Technische Hochschule Wildau (TH Wildau);
- Technische Universität Berlin (TU Berlin);
- Universität Potsdam.

In Ergänzung zu diesen Angeboten bereitet gegenwärtig das Georgius-Agricola-Institut (International School for Safety and Security) Bachelor- und Masterstudiengänge vor, die auf den Einsatz der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft orientieren. Die Besonderheit dieser Studiengänge ist die Einführung eines Fachvertiefungsprofils „Automation/Sicherheitstechnik“ mit folgenden Fachvertiefungsmodulen:
- Fachvertiefungsmodul 1: „Sicherheitsorientierte Aktor- und Sensorsysteme“

(Informationstechnische Strukturen, Prozessmesstechnik)
(Fertigungsmesstechnik);
- Fachvertiefungsmodul 2: „Prozess- und Gebäudesicherung/Safety“
(Prozessicherungssysteme)
(Requirement-Engineering für die Gebäudesicherung)
(Gebäudesicherungssysteme);
- Fachvertiefungsmodul 3: „Security“
(Security in der Automatisierungs- und Kommunikationstechnik)
(Security-Engineering);
- Fachvertiefungsmodul 4: „Qualitätssicherung/Zuverlässigkeit“
(Qualitätsmanagement)
(Zuverlässigkeit).

Literatur

Berlin Partner GmbH (Hg.) (2012): Die Sicherheitswirtschaft in Berlin und Brandenburg. Trends – Märkte – Potenziale. Auswertung einer Unternehmensumfrage 2011. Berlin. – URL: http://www.berlin.de/projektzukunft/fileadmin/user_upload/pdf/studien/umfrage_sicherheitswirtschaftbb_2011-12.pdf [27.04.2013]

BDSW – Bundesverband der Sicherheitswirtschaft (Hg.) (2012): Security Essen 2012: Der Sicherheitsmarkt in Deutschland. Zahlen, Daten und Fakten zur Branche. Essen. – URL: http://www.security-messe.de/media/presse_1/security_7/2012_14/3-Marktdaten~1.pdf [27.04.2013]

VAN – Virtual Automation Networks (ed.) (2010a): European R&D-Project “Virtual Automation Networks”. Final Report of Work package 11 “Project Management”. Nuremberg Moorenbrunn

VAN – Virtual Automation Networks (ed.) (2010b): European R&D-Project “Virtual Automation Networks”. Final Report of Work package 5 “Safety in Automation Systems”. Nuremberg Moorenbrunn

IPK – Institut für Produktionsanlagen und Konstruktionstechnik (2005): Abschlussbericht des Fraunhofer IPK im Rahmen des vom Berliner Senat geförderten FuE-Projektes „Sichere Produktion“. Berlin

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 123–124*

Mukayil Kilic, Klaus Fuchs-Kittowski

Sicherheitsrisiken und Vermeidungsverhalten im Fall der modernisierten und neuen Informationsquellen bei der Lenkung und Remotefunktionen von Fahrzeugen – Zusammenfassung

Im Zeitalter der Informations- und Kommunikationstechnologien (IKT) erhalten die Systeme für das Fahrzeug- sowie Flottenmanagement ihre Informationsqualität durch Erhöhung der Quantität der Informationsquellen. Je mehr Fahrzeuge, desto mehr Sensordaten, die verteilt sind. Aus diesen Daten generierte Informationen können gezielt bewertet und an die Interessenten zur Verfügung gestellt werden. Diese Informationen können z.B. Verkehrsleitsysteme versorgen.

Im Umkehrschluss kann das Verkehrsleitsystem über einen zentralen Knoten die Fahrzeuge mit Umwelt- und Umfeld-Daten versorgen oder lenken. Je mehr Sensoren es gibt und je ausgeprägter diese sind, desto besser wird die Qualität der gewonnenen Informationen sein. Es ist möglich, Bewegungsprofile z.B. für eine Stadt oder Region zu erstellen. Die Informationen werden durch die Vernetzung verstärkt und gewinnen dadurch neue Dimensionen. Die klassischen Verkehrsleitsysteme arbeiten im Gegensatz zu modernen Verkehr-Status-Anbietern mit fest installierten Sensoren. Diese Sensoren ermitteln u.a. die aktuelle Fahrzeuganzahl, Temperatur, Niederschlagsmenge, Luftfeuchtigkeit und Windgeschwindigkeit auf Autobahnen. Diese Informationen werden auf einem Server gesammelt und zur Verfügung gestellt. In diesem Modell ist eine flächendeckende Erfassung der Daten aus wirtschaftlichen Gründen nicht möglich.

Die gesammelten Informationen dienen als Grundlage für verschiedene Dienste. Besonders interessant sind unter anderem Geschwindigkeitsprofile. Es werden bereits Funktionen angeboten, die Geschwindigkeitsprofile für Kraftfahrtstraßen darstellen. Je mehr Personen diese Informationen zur Verfügung stellen, ihre GPS-Position und damit auch ihre Geschwindigkeit angeben, umso verlässlicher sind die daraus resultierenden Rückschlüsse. Staus

können so zeitnah erkannt und der Verkehr über passende Strecken umgeleitet werden. Der Dienst lebt also von seinen Nutzern.

Ein modernes Flugzeug könnte bei den hohen Geschwindigkeiten ohne IKT weder starten noch landen, und heutige Autos wären bei den Geschwindigkeiten auf der Autobahn ohne moderne IKT wahrscheinlich auch sehr unsicher. Durch den Einsatz der modernen IKT gewinnen wir also immer mehr Komfort und Sicherheit. Damit treten jedoch auf einer anderen Ebene neue Unsicherheiten auf (Paradoxie der Sicherheit).

Informationen können automatisiert aus den Fahrzeugen gesammelt werden. Die so genannten CAN-Botschaften (Controller Area Network), die auf dem CAN-Bus der Fahrzeuge für die fahrzeuginterne Kommunikation der einzelnen Steuergeräte dienen, werden über ein Kommunikationssteuergerät in Internetprotokolle umgewandelt. Nach dieser Transformation können unter Umständen „verschlossene“ Türen und Tore der deterministischen Fahrzeugkommunikation für die Allgemeinheit der Internetnutzer geöffnet werden.

Die jüngsten Updates für die TCP/IP-Bugs, die bis dahin unbekannt waren, leisten sicherlich einen schlechten Beitrag dazu. Denn den Informatikern ist bekannt, dass ein hundertprozentig sicherer Software-Test aus technischen Gründen ausgeschlossen, ein Korrektheitsbeweis für so komplexe Systeme nahezu unmöglich ist. In diesem Zusammenhang stellt sich die Frage: Wenn wir schon nicht die Internetprotokolle im Griff haben, welche Überraschungen erwarten uns dann in den darüber oder darunter liegenden Softwaresegmenten der Protokolle? Schon die unbekannten Risiken in den Internetprotokollen können zu großen Schäden führen.

Da ein Restrisiko nicht auszuschalten ist, bleibt unsere These, dass der Mensch gerade bei fortschreitender Automatisierung in letzter Instanz in der Verantwortung bleiben muss. Denn in riskanten Situationen kann er aufgrund komprimierter Erfahrung – Intuition – bei hoher Motivation und Qualifikation bessere Entscheidungen treffen als der Automat im formalen Bereich.

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 125–143*

Annely Rothkegel

Sicherheitskommunikation: Kommunikationskulturen im Kontext der Techniknutzung

1. Zum Thema

Der Begriff der Sicherheitskommunikation ist vielschichtig. Eine der Lesarten fokussiert auf Probleme der Sicherheit in einer Vielzahl von Domänen, Branchen und Disziplinen. Es wird gefragt, wie Sicherheit zu gewährleisten ist, z.B. durch Sicherheitstechnik oder Management.[1] Als in diese Lesart eingeschlossen gilt die Sicherstellung bzw. Absicherung von „kritischen Infrastrukturen" und Sicherung von Versorgungsketten um Großtechnologien wie Verkehrstechnologie, Energieversorgung, Informations- und Kommunikationstechnologie. Ziel ist die öffentliche bzw. zivile Sicherheit. Dieses Verständnis von Sicherheit wäre nach Banse (vgl. Banse 2011, S. 207) der Sicherheitsermöglichung zuzuordnen, die neben dem Sicherheitsbedürfnis das Konzept Sicherheit bestimmt.

Eine weitere Lesart fokussiert auf Probleme der Kommunikation selbst, und zwar mit der Frage, wie „gelingende" bzw. „gedeihliche" Kommunikation[2] zum Thema Sicherheit herzustellen ist. Diese Lesart steht in diesem Beitrag im Vordergrund, der sich damit in neuere kommunikations- bzw. medienwissenschaftliche Ansätze einreiht (vgl. u.a. Giebel 2012). Der Fokus des Beitrags liegt auf dem Umgang mit Sicherheit als Thema der Kommunikation. Dabei gehen wir von vier Sicherheitsmodellen aus, die sich semantisch durch das Verhältnis zu einem Ereignis (Unfall, Schadensfall, Katastrophe) unterscheiden.

1 Vgl. jährliche Veranstaltungen des Deutschen Städte- und Gemeindebundes gemeinsam mit der Alcatel-Lucent-Stiftung für Kommunikationsforschung zur „Bürgernahen Sicherheitskommunikation": URL: http://www.dstgb.de [29.04.2013].

2 „Gelingende" Kommunikation entspricht einer linguistisch-fachsprachlichen Formulierung im Sinne der Sprechakttheorie (vgl. Grice 1975) „gedeihliche" Kommunikation findet sich als Formulierung im ingenieurwissenschaftlichen Umfeld (vgl. Torgersen/Schmidt 2012, S. 113).

Als Bezugsrahmen für die Untersuchung kommunikationsbezogener Phänomene bietet sich das Konzept der Kommunikationskultur an (vgl. Hribal 1999; Maier-Rabler/Latzer 2001). Angepasst an Phänomene der sprachlichen Kommunikation bilden Akteure und deren Interaktionen, der situative Kontext sowie die Themenentfaltung die relevanten Komponenten von Kommunikationskulturen. In diesem Beitrag steht die Themenentfaltung im Vordergrund. Sie gilt als vorgeprägt durch das jeweilige Sicherheitsmodell, das in der Interaktion der Beteiligten zum Tragen kommt. Die linguistisch-semantische Explizierung von Modell und thematischer Entfaltung erfolgt in Form von Begriffsfeldern, die Beschreibung wie auch Unterscheidung und Vergleich gestatten. In diesem Sinne ist eine Typologie von Kommunikationskulturen anvisiert, die hier exemplarisch anhand von vier Typen unterschieden werden (Abschnitt 4). Dieser Skizze geht eine Vorstellung der Konzepte Kommunikationskultur (Abschnitt 2) und Sicherheitsmodell (Abschnitt 3) voraus. Im Fazit (Abschnitt 5) wird auf den Zusammenhang von Kommunikationskulturen und Sicherheitskulturen hingewiesen. Den begrifflichen Hintergrund bilden Ansätze der Sicherheitsforschung (vgl. u.a. Bonß 2010; Winzer et al. 2010) und Sicherheitskommunikation (vgl. Giebel 2012).

2. Kommunikationskulturen als Basis der Sicherheitskommunikation

Kommunikationskulturen spiegeln eine spezifische Konfiguration kommunikativer Parameter, die für eine Gruppe (Kollektiv) von Menschen als nichthinterfragte Gewohnheiten selbstverständliche Geltung haben (vgl. Hansen 2011).[3] In unserem Ansatz betrachten wir die Kommunikation als eine Ebene, auf der kulturelle Parameter in den Äußerungen selbst sichtbar und somit als Indikatoren textanalytisch zugänglich sind.[4]

Grundlage unseres Ansatzes bildet die Zuordnung von Realsituation und der durch sie ausgelösten Kommunikationssituationen. Zur Kennzeichnung der Realsituation dienen das (unerwünschte) Ereignis und die Reaktion darauf in Form von Maßnahmen. Die Kommunikationssituation ist gekennzeichnet durch das Thema und dessen Entfaltung auf der Grundlage eines Sicherheits-

3 Hansen verbindet den Kulturbegriff einerseits mit den Gewohnheiten von Gruppe, Kollektiv oder Gesellschaft („Kultur bedeutet kollektives Gleichverhalten"; Hansen 2011, S. 29), andererseits mit dem Begriff der Standardisierung, der im Hinblick auf die Kommunikation mit dem Gebrauch von Zeichensystemen in Verbindung gebracht wird, die die Konstruktion von Bedeutung (z.B. in begrifflichen Systemen) regeln.

4 Gemeint sind thematische Begriffsfelder, die aus Platzgründen hier nur angedeutet werden können.

modells sowie durch den Typ der Interaktion mit den dominanten Sprachhandlungen zwischen den Kommunikatoren. Kommunikation ist verstanden im Sinne einer interpersonalen Kommunikation, bei der die Beteiligten aufeinander einwirken. Anders als bei der Vorstellung vom linearen (Wissens-) Transfer von A nach B ist die Interaktion offen für unterschiedliche Verständnisse sowie für mögliche kognitive Veränderungen der Beteiligten.

3. Basismodelle zum Sicherheitsverständnis

3.1 Was sind Modelle und wozu taugen sie?

Wegen der gegenüber der Realität reduzierten Komplexität sind Modelle geeignet für Planungen, Untersuchungen, Simulationen oder Trainings, die am Original nicht möglich oder unkomfortabel sind. Bei der Entwicklung von technischen Produkten spielen sie eine wichtige Rolle, z.B. im Bereich von Bionik, Robotik, Prothesenherstellung oder Softwareentwicklung (vgl. Dutke 1994; unter sprachlichen Gesichtspunkten vgl. Jacob 1991). Mentale Modelle, in der Sicht der Kognitionswissenschaften (vgl. Johnson-Laird 1983; zur kognitiven Linguistik vgl. Schwarz 2008), sind gedanklicher Art und können verstanden werden als Sichtweisen auf die „Welt“. Sie haben zu tun mit dem Wissensstand und den Einstellungen von Personen, nach denen das „Bild“ von der Realität gefiltert wird (z.B. „unterschiedliche Weltbilder“ in der Biotechnologie-Debatte; vgl. Gill 2012, S. 65). Modelle beeinflussen nicht nur die Denkweise der Akteure, sondern auch deren Handeln und haben dabei den Status von Strategien.

In unserem Ansatz gehen wir von vier Basis-Modellen der Sicherheit aus (zu Details vgl. Rothkegel 2010b). Gemeinsamer situativer Bezugspunkt ist ein (unerwünschtes) *Ereignis*, als zentral gelten die weiteren Schlüsselbegriffe *Risiko*, *Gefahr*, *Abwehr*, *Schutz*. Wir unterscheiden folgende Zuordnungen: (1) Sicherheit = kein Risiko, keine Gefahr, (2) Sicherheit = Umgang mit Risiko, (3) Sicherheit = Umgang mit Gefahr durch *Abwehr* und/oder (*externen*) *Schutz*, (4) Sicherheit = (*interner*) *Selbstschutz* (Robustheit, Resilienz).

3.2 Modell „Sicherheit = kein Risiko, keine Gefahr“

Die Bedeutung von „Sicherheit“ als Alltagsbegriff, wie sie im Bedeutungswörterbuch „DUDEN“ dargestellt ist (vgl. DUDEN 2002), umfasst mehrere Lesarten, von denen lediglich zwei in unserem Zusammenhang relevant sind. Es geht um die Lesart „Sichersein vor Gefahr oder Schaden“, mit dem Syn-

onym „Schutz“ sowie um die Lesart „Freisein von Fehlern oder Irrtümern“.[5] Daneben gibt es im Weiteren die „Sicherung“ im Sinne von Absicherung, z.B. Friedenssicherung, auch in Komposita wie Energiesicherheit. Im (auch wissenschaftlichen) Sprachgebrauch und Verständnis der Kommunikatoren mag es zu Mischungen kommen.[6] Das immer wieder geäußerte Stereotyp, dass es „keine 100-prozentige/absolute Sicherheit“ gebe, bezieht sich also auf die alltagssprachliche Lesart.[7]

3.3 Modell „Sicherheit = Umgang mit Risiko“

Die Spezifikation von „Risiko“ ist theoretischer Art, d.h. die Bedeutung hängt grundsätzlich von der Theorie und damit von der Disziplin ab, in der sie entwickelt wird (Risiko als Konstruktion; vgl. Becker 1993). Die Risikoforschung, insbesondere als Reaktion auf eine Reihe technischer Großunfälle in den 1980er Jahren, hat sich ausführlich um eine systematische Sortierung der Begrifflichkeiten bemüht (vgl. Banse 1996). Diese Arbeiten sind zu sehen innerhalb einer generellen Aufmerksamkeit für die Zunahme von Risiken sowie Anfällig- und Verletzbarkeiten (*vulnerability*) moderner Gesellschaften durch jegliche Art von Katastrophen (vor allem soziologische Ansätze; vgl. Beck 1986, 2010; Bonß 1995; Luhmann 1991).

In naturwissenschaftlich-technischer Perspektive unterscheidet man Risiken, die als kontrollierbar bzw. nicht-kontrollierbar eingestuft werden. Hierbei geht es um konkrete festgelegte Maßnahmen (Kontrolle) im Umgang mit definierten Gefahren. Als attraktiv gilt in diesem Zusammenhang das Verständnis vom Risiko als Kalkül. Es liefert eine Grundlage für die berechenbare Einschätzung eines Risikos. Die Berechnung bezieht sich dabei auf das Verhältnis von Eintrittswahrscheinlichkeit eines Schadensereignisses und dem Ausmaß des Schadens.

„Risiko“ ist grundsätzlich auf Zukunft ausgerichtet, Aussagen darüber orientieren sich an Wahrscheinlichkeiten und Prognosen, wobei unsicheres Wissen und Ungewissheiten zu berücksichtigen sind. Insofern spielen weitere Begriffe wie Akzeptanz bzw. Nicht-Akzeptanz eine Rolle (vgl. Grunwald 2005). Die jeweiligen Zuordnungen sind abhängig von den beteiligten Indi-

5 Die anderen Lesarten entsprechen Synonymen wie *Gewissheit*, *Zuverlässigkeit*, *Selbstsicherheit*, *Bürgschaft*. Diese Lesarten spielen in unserem Zusammenhang keine Rolle.

6 So beziehen sich Beyerer et al. (2010, S. 39) auf die emotionale Einstellung der beteiligten Personen und deren Verständnis von Sicherheit im Sinne der „Abwesenheit von Furcht vor Gefahren“.

7 Sie kann aber auch im fachlichen Kontext vorkommen: „Es gilt aber festzustellen, dass eine absolute Sicherheit theoretisch nicht erreicht werden kann“ (Fratzscher 2011, S. 138).

viduen, Gruppen, Organisationen. Dabei werden, soziologisch gesehen, Akteure im Sinne von Risikoproduzenten und Entscheidern sowie Betroffene unterschieden. Unter ökonomischen Gesichtspunkten verbinden sich mit dem Begriff des Risikos bestimmte Vorstellungen von Situationen, in denen Ereignisse oder Handlungen einen Vorteil (Nutzen) und/oder Nachteil (Schaden) bringen. Man geht das Risiko eines Schadens ein (Risikobereitschaft), wenn man gleichzeitig an einen Vorteil und das Nicht-Eintreffen des Schadens glauben kann oder wenn der Nutzen den erwarteten Schaden überwiegt. In diesem Zusammenhang kommt der Begriff vom „Wagnis" ins Spiel (vgl. Beyerer et al. 2010, S. 52).

3.4 Modell „Sicherheit = Maßnahmen von Abwehr und Schutz"

Das Abwehr-Schutz-Modell orientiert sich am Schlüsselbegriff der „Gefahr", d.h. das Ereignis ist im Hinblick auf sein Gefährdungs- oder Bedrohungspotenzial spezifiziert (vgl. Münkler et al. 2009; Schirmer 2008). Diese wie die grobe Zuordnung der Maßnahmen von Abwehr und Schutz kennzeichnen die Sicherheitsforschung, die die Risikoforschung abgelöst hat, wie auch die Praxis der letzten Jahre.[8] Eine Brücke zwischen den beiden Kernbegriffen Risiko und Gefahr ergibt sich, wenn Sicherheit verstanden wird als „Abwesenheit eines unvertretbaren Risikos und Gefahr als Anwesenheit eines unvertretbaren Risikos" (vgl. Regenfuß/Viehweg 2010, S. 132, in Anlehnung an DIN Fachbericht 144 zur Sicherheit).

Wichtig ist die Gefahrenquelle, die schädigend auf eine andere Einheit einwirkt und deshalb für sie eine Bedrohung (engl. *hazard*) darstellt.[9] Betrachtet man die Techniknutzung als Interaktion zwischen Akteur, technischem System und Umwelt[10], kommen alle drei gleichermaßen als Gefahrenquelle wie auch als Opfer in Frage. Akteure können Fehler machen (in der Konstruktion oder bei der Bedienung mit „menschlichem Versagen") oder als „böse" Angreifer Technik für die Schädigung anderer missbrauchen (Attacke, Anschlag, Sabotage). Technische Systeme bilden Gefahrenquellen auf verschiedenen Ebenen. Dabei ist grundsätzlich das systeminterne Gefah-

8 Einen Überblick zur Forschungslage vermittelt der von der Deutschen Akademie der Technikwissenschaften (acatech) herausgegebene Sammelband „Sicherheitsforschung – Chancen und Perspektiven" (vgl. Winzer et al. 2010); darin ist ein Überblick über nationale und internationale Forschungsprogramme (vgl. Thoma et al. 2010, S. 14-27); vgl. des Weiteren Giebel 2012; Stieniczka 2006.

9 Beispiel: Art der Bedrohung = Elektrizität (bzw. austretendes Gas), Schaden = Stromschlag (bzw. Vergiftung).

10 Also eine Erweiterung des soziotechnischen Systems im Sinne von Günter Ropohl (vgl. Ropohl 2009).

renpotenzial zu beachten.[11] Aber auch Defekte (durch Transport oder Gebrauch) können zur Gefahrenquelle werden,[12] oder es geht um das Versagen von Kontrollmechanismen („technisches Versagen"). Einwirkungen aus der Umwelt wiederum, denen in der Konstruktion oder mit der Einschränkung von Gebrauchsweisen Rechnung getragen wird, können sich der Kontrolle teilweise oder gänzlich entziehen.[13] Auf der Grundlage solcher Basiskomponenten ergeben sich eine Reihe denkbarer Konfigurationen, die als Gefahrensituationen erfasst werden können.

Die zu bestimmenden Maßnahmen operieren in zwei Richtungen. Einerseits geht es um Abwehrmaßnahmen hinsichtlich der Gefahrenquellen, andererseits um Schutzmaßnahmen in Bezug auf die potenziellen Schadensobjekte (Lebewesen, Sachobjekte, Natur, Infrastrukturen). Wichtig sind Vermeidung, Verhinderung oder zumindest Verringerung von Schaden (Prävention). Tendenziell und vom Konzept her geht man davon aus, dass die Gefahr kontrolliert und Schaden vermieden werden kann. Bei den Schutzmaßnahmen geht man dagegen davon aus, dass nicht alle Gefahren abgewendet werden können. Dabei sollen die Betroffenen und vor allem die Einsatz- bzw. Rettungskräfte aber soweit möglich vor den Folgen geschützt werden (z.B. durch Schutzanzüge bei Bränden oder KKW-Störfällen).

Der Gegenüberstellung von Abwehr und Schutz entspricht die Gegenüberstellung von aktiver und passiver Sicherheit. Im Kfz-Bereich spricht man von aktiver Sicherheit, wenn die Vorrichtungen in spezifischer Weise auf bestimmte Gefahren hin konstruiert sind, so etwa Bremssysteme oder Fahrspur-Assistenten. Passive Sicherheit hat dagegen mit der Schadensbegrenzung bei einem Unfall zu tun, so etwa die Verwendung von Gurten (rechtlich unterstützt durch Anschnallpflicht) oder von Airbags. Norbert Stieniczka verfolgt auf eindrucksvoll belegte Weise, wie sich das vormalig vorherrschende Verständnis von aktiver Sicherheit in den 1970/80er Jahren in der BRD langsam zu einem Denken in Kategorien passiver Sicherheit wandelte (vgl. Stieniczka 2006).[14]

---

11 Z.B. Elektrizität, Gefahrenstoffe, Bewegungen von Robotern, Kernschmelze.

12 Z.B. beim Kühlgerät das Austreten von Kühlmittel aufgrund einer Beschädigung des Behälters.

13 Z.B. Wetterverhältnisse bei der Nutzung von Verkehrsmitteln.

14 In der Sicht aktiver Sicherheit herrscht die Meinung vor, dass mit technischen Mitteln Schaden verhinderbar ist, d.h. dass ein Ereignis nicht stattfinden kann (z.B. durch geeignete Bremssysteme); in der Sicht passiver Sicherheit geht man davon aus, dass Ereignisse zwar stattfinden, dass der Schaden aber durch technische Mittel abgewendet bzw. klein gehalten wird (z.B. durch Gurtsysteme).

Eine weitere Gegenüberstellung betrifft die Konzepte von „safety“ und „security“, die im deutschen Ausdruck in der gleichen Benennung „Sicherheit“ verwendet werden, von ihrer begrifflichen Bedeutung aber gleichwohl unterschieden sind. In einer groben Unterscheidung bezieht sich „safety“ auf die Betriebssicherheit (Funktionsfähigkeit), während „security“ auf intendierte Schadensereignisse abzielt, der in der Forschungslandschaft mit Blick auf die zivile Sicherheit eine hervorgehobene Rolle zukommt.

Anders als in der Perspektive einer Gefährdungssituation stellt sich dieselbe Situation in der Perspektive einer Schutzsituation dar. Diese Sichtweise kennzeichnet das „Produktsystem Sicherheit“, das mit drei Rollen der Beteiligten (Personen wie auch Objekte sowie Prozesse und Strukturen) beschrieben werden kann (vgl. Beyerer et al. 2010, S. 40): Es gibt Schutzbedürftige (Personengruppen, technische Systeme), Gefährder und Schützer. Sicherheit wird verstanden als Dienstleistungsbeziehung zwischen Schutzbedürftigem und Schützer. Als Gefährder kommen, wie im konventionellen Abwehr-Schutz-Modell, sowohl technische Defekte (nicht-intendierte Gefährdung) wie auch Terroristen (intendierte Gefährdung durch Angreifer) in Betracht.

3.5 Sicherheit = Selbstschutz im Sinne von Robustheit und Resilienz

Selbstschutz umfasst Maßnahmen, bei denen sich wiederum zwei Orientierungen unterscheiden lassen: der Bezug auf Schwachstellen (Robustheit) oder Stärken (Resilienz) eines (biologischen, sozialen, technischen) Systems. Bei technischen Systemen gehören Betrachtungen hinsichtlich möglicher Schwachstellen zu den Standards der Qualitätssicherung. Bei den Schutzmaßnahmen gibt es Überlappungen zum Safety-Bereich, insofern als die „Flanken“ eines Systems bearbeitet werden.[15] Entsprechend stehen Maßnahmen der „Härtung der verwundbaren Flanken“ (Beyerer et al. 2010, S. 43) im Vordergrund. In diesem Sinne stehen sich Robustheit und Verwundbarkeit (Vulnerabilität) als Antonyme gegenüber. Bei Robustheit geht es um Antizipation und Anwendung bekannter Routinen.[16]

Anders verhält es sich beim Begriff der Resilienz. In der Überblicksdarstellung zur Sicherheitskommunikation von Giebel (vgl. Giebel 2012, S. 89-

15 Flanke im Sinne einer Metapher aus dem Tierbereich (leicht verletzbare Bauchseite) bzw. bereits metaphorisiert im militärischen Bereich angewendet mit Bezug auf die beiden (leicht angreifbaren) Außenseiten der Aufstellung.

16 Im Bereich der System- und Prozessgestaltung ist mit Robustheit gemeint, dass ein System Veränderungen von außen standhält und nach einer Irritation wieder in seinen Ausgangszustand zurückkehrt.

94) werden die verschiedenen Positionen zum aktuell diskutierten Resilienzbegriff referiert, wobei durchgängig die Dynamik und Ungewissheit der beachteten Situationen hervorgehoben werden. Der Unterschied zum Begriff der Robustheit wird am Ereignis festgemacht (vgl. Giebel 2012, S. 91): Während Robustheit sich auf ein fixes Ereignis, eine identifizierte Störung bezieht, ist Resilienz offen für Irritationen jeglicher Art, also auch für überraschende, unerwartete Ereignisse.

Der Begriff der Resilienz wandert in den letzten Jahren durch die verschiedenen Disziplinen und wird entsprechend differenziert paraphrasiert (vgl. u.a. Brand/Jax 2007; Folke 2006; Gabriel 2005). In der Physik bzw. Materialwissenschaft spricht man von Elastizität, in der Medizin, wo das Konzept seinen Ursprung haben soll, von Widerstandsfähigkeit, in der Psychologie vom Vermögen, Lebenskrisen ohne anhaltende Beeinträchtigungen durchzustehen (vgl. Giebel 2012, S. 90). In der Grundbedeutung ist Resilienz demnach generell zu verstehen als eine Fähigkeit sowie das Verfügen über Ressourcen für adäquate Reaktionen auf Unsicherheiten, d.h. „Leben mit Risiko“ (vgl. Bohle 2008).[17]

4. Sicherheit als Thema von Kommunikationskulturen

4.1 Erlebnis statt Ereignis: Wenn Sicherheit kein Thema ist

In einer positiven Erwartungshaltung („Technik als Erwartung“; vgl. Kaminski 2010) ist die Sicherheitsrelevanz gering. Die Zukunftsorientierung begünstigt ein Verständnis von Sicherheit im Sinne der Alltagsbedeutung („keine Gefahr“). An die Stelle eines möglichen unerwünschten Ereignisses tritt ein erwünschtes Erlebnis (zum Konzept der Erlebnisgesellschaft vgl. Schulz 1992). In der daraus ausgelösten Kommunikationssituation ist kein Raum für das Thema Sicherheit. Den Darstellungen liegen Technikmodelle zugrunde, die für Fortschritt und das Wunderbare stehen. So finden sich im Zusammenhang mit Wissenschafts- und Techniksendungen, z.B. in den Medien, stereotype Formulierungen wie „Faszination Technik“ oder „Wunder der Technik“. Dies ist eine Tradition, die ins 17. Jahrhundert zurückgeht, wo Technik zur Imageförderung der Fürsten entwickelt und öffentlich zur Schau gestellt (vgl. Lazarding 2006) oder im 19. Jahrhundert Bestandteil der neuen Unterhal-

17 Dazu gehören (zitiert nach Daniela Giebel; vgl. Giebel 2012, S. 94): Prävention (to prevent something bad from happening), Proaktion (to prevent something bad from becoming worse), Reaktion (to recover from something bad once it has happened).

tungskultur wurde (vgl. Weber 2006). Auch in der historischen Perspektive der Technikgeschichtsschreibung stehen die jeweils neuen technischen Errungenschaften im Sinne von Fortschrittsgläubigkeit und Zukunftsorientierung in der Regel im Vordergrund (zu „Ursprüngen der Zukunft" vgl. Metz 2006; zu alternativen Sichtweisen vgl. Neubert/Schabacher 2013).

Der Blick in die Zukunft scheint erst recht eine quasi euphorische Einstellung zu fördern. Insofern als Prognosen oder Visionen ausschließlich in der Kommunikation existieren, kann es leicht vorkommen, dass fehlendes Erfahrungswissen durch Wunschdenken ersetzt wird. In der Gegenwart, in der Aspekte des Marketings dominieren, werden häufig Information und Werbung vermischt, wobei Letzteres am Sprachgebrauch erkennbar ist. Ein Beispiel dafür liefert der „Science Express", ein von der Max-Planck-Gesellschaft initiiertes und gefördertes Projekt mit Ausstellungszug, der 2009 als „Expedition Zukunft" an etlichen deutschen Bahnhöfen die Öffentlichkeit (vorwiegend in Bildern) darüber informierte, „wie Wissenschaft und Technik unser Leben verändern" (vgl. MPG 2009).[18]

Zusammenfassung: Beobachtbar ist eine Kommunikationskultur, in der Realsituationen nicht mit dem Thema Sicherheit in Verbindung gebracht werden. Anstelle des Ereignisses tritt das Erlebnis. Dies gibt Raum für Technikdarstellungen, die einerseits der Attraktivität technischer Lösungen gerecht werden, fördert andererseits Wunschdenken und Spekulationen, die sich allerdings gut vermarkten lassen. Die Interaktion bezieht sich auf die öffentliche Vermittlung. Sie ist gekennzeichnet durch einen Mix von Handlungen des Informierens, Ankündigens, Versprechens und Werbens. Als Reaktionen werden Interesse (Aufmerksamkeit), Begeisterung (Attraktion) und Bewunderung (Faszination) erwartet.

Zum typischen Begriffsfeld gehören neben Stereotypen wie *rasante Entwicklung*, *Wunder*, *Faszination* neutrale Ausdrücke wie *Innovation*, *Fort-*

18 Eine Vermenschlichung von Technik ist zu beobachten, wenn gezeigt wird, „wie Robotern Leben eingehaucht wird" (S. 93), wie das Internet uns unterstützt als „persönlicher Assistent, Berater, Weg- und Lebensbegleiter" (S. 110) und wie „ein neues Zeitalter der Medizin anbricht" (S. 163), in dem die Frage gestellt werden kann „Wird es eine Welt ohne Krankheiten geben?" (S.163) und in dem „Ingenieure die neuen Halbgötter in Weiß werden" (S. 164). Das hiermit ausgedrückte Technikmodell ordnet Karl H. Metz einer 2. Phase der Technikentwicklung zu („in der das Menschenhafte ganz im Zentrum steht"), während die 1. Phase den Gegensatz zur Natur hervorhebt, die 3. Phase als „absolute Technik" unabhängig von beiden ist und sich der Kunst annähert, was in der Kunstrichtung des Futurismus Programm geworden ist (vgl. Metz 2006, S. 549).

schritt, *Moderne* und weitere Begriffsfelder aus den jeweiligen Domänen bzw. „Erlebniswelten".

4.2 Kommunikationskultur der Kontroverse um das Risiko

Wie spricht man über Risiken in der Öffentlichkeit? In Abschnitt 3.3 war auf den theoretischen und fachbezogenen Status des Begriffs Risiko hingewiesen worden. In der Öffentlichkeit sind neben der technischen Fachwelt viele andere Gruppen beteiligt: Nutzer, Verteiler, Interessengruppen, Anspruchsgruppen, Behörden, Politiker, Bürger als Betroffene im weitesten Sinne. Mit der Sicht auf Technik in der Nutzung kommen viele und sehr verschiedene Kontexte in den Blick, die zusätzlich zu den technischen Fakten Argumente aus anderen Bereichen der Lebenswelt in die Kommunikation einbringen (z.B. Gesundheit, Umwelt, Markt, Politik). Die Rede ist von der „De-Fokussierung technisch-naturwissenschaftlicher Fragen" (Boysen 2012, S. 16). Die Kommunikation ist geprägt durch Merkmale der Experten-Nichtexperten-Kommunikation, d.h. den Mix von Fach- und Alltagswissen sowie von Fach- und Alltagssprache und den damit verbundenen Kommunikationsproblemen. So kommt es leicht zu einer Polarisierung, wobei den Medien eine spezifische Rolle zugeschrieben wird. Die Rede ist von „securitainment" und Inszenierung von Sicherheit (vgl. Andrejevic 2011; Bidlo/Englert 2009). In diesem Sinne erscheint die mediale Risikokommunikation als Kommunikationsrisiko (vgl. Bechmann/Stehr 2000; Krüger/Ruß-Mohl 1991; Obermeier 1999).

Dem steht der Versuch gegenüber, in einer als Dialog (und nicht einseitigen Informierung) verstandenen Kommunikation die unterschiedlichen Positionen als solche zu klären. Ein Beispiel ist die Diskussion zum Thema der Biotechnologie-Kommunikation, die im Rahmen der Akademie der Technikwissenschaften im Oktober 2011 stattgefunden hat (vgl. Weitze/Pühler 2012).

Unabhängig von einem Pro oder Contra zur Biotechnologie (Pro für die Rote [Medizinbereich] und Contra für die Grüne [Agrarbereich]; vgl. Boysen 2012) verdeutlicht die acatech-Diskussion, welche Aspekte des Risikomodells die Kontroversen bestimmen. Dabei stehen sich Fach- und Erfahrungswissen gegenüber. Auf der einen Seite geht es um „Kontrolle" bzw. „Kontrollierbarkeit" durch Berechnung von Wahrscheinlichkeiten (Eintritt und Schadenshöhe von Ereignissen), auf der anderen um „Erfahrungswissen". Ein hervorgehobenes Thema betrifft Fragen der „Relevanz" (Gibt es Alternativen, gibt es Notwendigkeiten?). Außerdem erhalten Themen wie Nutzen und Schaden öffentliche Aufmerksamkeit, die die Debatten auf einer Skala zwischen Akzeptanz und Ablehnung bewegen.[19] Hier zeigt sich deut-

lich, dass Risikowahrnehmung und Risikoeinschätzung stark von den lokalen Gegebenheiten wie den Interessen der jeweiligen Gruppierungen abhängen (zu einer kritischen Einschätzung vgl. auch Rifkin 2003).

Aufgrund der prinzipiellen Zukunftsorientierung und Offenheit von Prognosen erscheinen die Versprechen der Risikoproduzenten zwangsläufig mit deren Glaubwürdigkeit gekoppelt. Ohne allseitig begründete Vertrauensbasis kann in diesem Kontext keine gelingende Kommunikation stattfinden (vgl. auch Renn 2010).[20] In diesem Sinne erscheint die Kommunikationskrise im Hinblick auf das Thema Grüne Biotechnologie eher als Vertrauenskrise denn als Mangel an Informationsvermittlung.

Zusammenfassung: Eine Kommunikationskultur, in der der Begriff des Risikos die Sicherheitskommunikation bestimmt, ist per se konflikthaft. Vor dem Hintergrund von Fach- und Erfahrungswissen bilden sich unterschiedliche Situationseinschätzungen. Die Interaktion ist geprägt durch Kontroversen, die Beziehungsebene, insbesondere mit dem Merkmal Vertrauen, gewinnt an Gewicht. Die kommunikativen Handlungen umfassen in erster Linie argumentative Strategien, teilweise mit kämpferischem Tenor.

Zum elaborierten Begriffsfeld gehören u.a. *Risiko* (*R-wahrnehmung, R-analyse, R-identifikation, R-einschätzung, R-bewertung, R-Minimierung, R-Kompensation*); in Bezug auf das Ereignis*: Eintrittswahrscheinlichkeit*, *Schaden*, *Verlust, Kosten, Schadenshöhe*, *Nutzen, Gewinn, Chancen*; in Bezug auf Maßnahmen: *Entscheidung, Wagnis, Relevanz, Alternativen;* in Bezug auf die Interaktion: *Vertrauen, Glaubwürdigkeit, Akzeptanz, Nicht-Akzeptanz*.

4.3 Kommunikationskulturen der Techniknutzung in der Praxis: zur Darstellung von Abwehr- und Schutzmaßnahmen

Gängig ist, dass zunächst eine Technologie entwickelt und dann in die Praxis entlassen wird, wo sich entscheidet, ob sie im Kontext der Anwendung funk-

19 So wird u.a. in dem genannten Sammelband mehrfach betont, dass der mögliche oder versprochene medizinische Vorteil/Nutzen (wissenschaftlicher Fortschritt) die Akzeptanz für die Rote Biotechnologie (Medizinbereich) bei den Nichtexperten begünstigt, während man hinsichtlich der Grünen Biotechnologie (Agrarbereich) tendenziell keine Akzeptanz aufbringt, weil, so die Argumentation (der Bauern als Nutzungsexperten), diese unnötig sei und keinen Nutzen bringe (zu den unterschiedlichen Ausgangssituationen in den USA und Europa vgl. Bonfadelli 2012, S. 217f.).

20 Heinz Bonfadelli verweist in diesem Zusammenhang auf die aktuelle Situation in der Schweiz, wo derzeit keine Debatte (mehr) stattfindet, was er bezeichnenderweise als „Kampfpause“ interpretiert (vgl. Bonfadelli 2012, S. 211).

tioniert und akzeptiert wird. Mit dem zweiten Schritt wird aus dem technischen Produkt ein Objekt in einem sozialen Feld, das sich charakterisieren lässt durch jeweils eigene Voraussetzungen und Bedingungen, durch Akteure in verschiedenen Rollen sowie im Hinblick auf mögliche und tatsächliche Folgen auf verschiedenen Ebenen (ökonomisch, psychologisch, sozial, kulturell). Der Übergang vom technischen Konstrukt zum soziotechnischen System (vgl. Ropohl 2009, S. 141) wird begleitet wie auch beeinflusst durch Kommunikation. Dabei spielt das Thema Sicherheit eine ganz wichtige Rolle. Es geht um konkrete Maßnahmen, in die die Nutzer wesentlich und individuell sowie mit allen Folgen involviert sind. Im Zentrum stehen Maßnahmen der Abwehr der Gefahren und des Schutzes der potenziellen Schadensobjekte, bei denen Gesetzgebung und Normen nicht nur für Standards sorgen, sondern auch einschränkend in Verhalten und Bewegungsfreiheit von Personen eingreifen.

Durch die zwei grundsätzlich unterschiedlichen Typen von Realsituationen werden entsprechend unterschiedliche Kommunikationssituationen ausgelöst. Einmal geht es um die Ausführungshandlungen bei der Nutzung von technischen Produkten, die in den Anleitungstexten und insbesondere in den so genannten Sicherheitshinweisen thematisiert werden. Für diese Fälle kann man eine Art „compliance“ der Nutzer unterstellen, da sie an einem erfolgreichen Ergebnis interessiert sind. Probleme beziehen sich in erster Linie auf Verständlichkeit und Verstehen (vgl. Hennig/Tjarks-Sobhani 1999). Ein andermal geht es um Abwehr von und Schutz vor Attacken, an denen die Nutzer zwar ebenfalls interessiert sind, wo es aber Spielräume in der Wahl der Maßnahmen gibt. So können hier ebenfalls konflikthafte Debatten entstehen, in denen Sicherheit versus Freiheit eine Opposition bilden (vgl. Münkler 2010).

Neben diesen öffentlich stark beachteten Situationen geht es in der professionellen wie privaten Alltagspraxis um weniger beachtete (bzw. ungelesene), aber sehr häufige Texte, die den typischen Umgang mit Technik thematisieren: die Technische Dokumentation und Ratgeber. Gemeinsam ist ihnen der Bezug auf Situationen, in denen der individuelle Umgang mit einem technischen Produkt in einen übergreifenden Handlungskontext mit anvisierten Zielen eingebunden ist. Derartige Ziele lassen sich als Aufgaben beschreiben, wobei Ausgangspunkt und erwünschtes Ergebnis feststehen. Dieser Zusammenhang bildet in der Regel das Thema von Gebrauchsanleitungen (als Anleitung zur Anleitung vgl. Juhl 2005).

Interessant ist, dass in den obligatorischen Sicherheitshinweisen eine Welt in der Negation konstruiert wird: Szenarien, die „nicht sein sollen“ (z.B.

Finger und Gegenstände gehören nicht ins Geräteinnere; vgl. Rothkegel 2010a, S. 63). Hierzu existieren Normen über Inhalte und Formulierungen, insbesondere in den USA und der EU (ANSI, DIN, ISO/EN).[21] Die Ratgeberliteratur, insbesondere im Bereich der IT-Sicherheit, beschäftigt sich in erster Linie mit Tipps für Abwehr- und Schutzmaßnahmen gegen Attacken (vgl. Campo 2001). Technische Systeme können dabei das Ziel sein (Blockierung von Servern mit allen Folgen) wie auch das Mittel (z.B. Software wie Viren, Würmer, Trojanische Pferde). Typisch für die Ratgeber-Literatur ist, dass Attacken ähnlich wie Fehler typisiert und beschrieben und damit den Sicherheitslücken im technischen System zugeordnet werden. Was persönliche Beschränkungen betrifft, spricht man von einer „Einschränkung des Benutzerkomforts" (Campo 2001, S. 22). Die Opposition ist hier Sicherheit versus Komfort.

Zusammenfassung: Gefahren bzw. Gefährdungen/Bedrohungen stehen im Fokus einer Kommunikationskultur, in der Sicherheit im Sinne von konkreten Maßnahmen der Gefahrenabwehr bzw. des Schutzes potenzieller Schadensobjekte verstanden wird. Das Ereignis selbst, das die Gefahrensituation bestimmt, gewinnt eine große Bedeutung in der Kommunikation. Das Spektrum der Möglichkeiten ist groß und vielfältig. Es reicht von der Nutzung technischer Produkte im Alltag bis zu groß angelegten intendierten Attacken. Die Kommunikation selbst bildet einen Bestandteil der Maßnahmen, wofür es rechtliche und dokumentarische Standards gibt. Im Hinblick auf die Interaktion stehen Handlungen des Informierens, Instruierens sowie Warnens und Ratgebens im Vordergrund (zum Warnen vgl. Dombrowsky 2005).

Zum elaborierten Begriffsfeld gehören u.a. *Sicherheit: safety/security*, *aktive und passive Sicherheit*, *Sicherheitslücken, Sicherheitsniveau*; in Bezug auf das Ereignis: *Schadensereignis*; nicht-intendiert: *Fehler*; intendiert: *Attacke, Angriff, Missbrauch, Sabotage, Spionage*; in Bezug auf die Gefahr: *Gefahr*, *Gefährdung*, *Gefahrenpotenzial*, *Gefahrenquelle*, *Gefahrenabwehr*; zur Abwehr: *Gefahrenabwehr*, *Prävention*; zum Schutz: *Schutzobjekt, Schadensobjekt, Schadensziel, Vorsorge, Rettung*.

21 Drei Dimensionen einer Gefahrensituation werden standardmäßig berücksichtigt: Aufmerksamkeitslenkung, Warnung durch Angabe der Gefahrenquelle und Angabe des möglichen Schadens, Ratschlag bzw. Empfehlung hinsichtlich notwendiger oder nützlicher Maßnahmen. Neben den Standardsituationen sind Differenzierungen von Gefahrensituationen denkbar, z.B. im Hinblick auf das systeminterne Gefahrenpotenzial, einen Defekt, eine nicht oder nur teilweise kontrollierbare Einwirkung von außen, einen Fehler in der Bedienung, einen Missbrauch in der Nutzung (vgl. Rothkegel 2011, S. 278-280).

4.4 Kommunikationskultur des Trotzdem: Selbstschutz durch Robustheit und Resilienz

Eine andere Prägung charakterisiert die Kommunikationskultur, wenn es hervorgehobene Eigenschaften und Fähigkeiten eines Systems sind, die die Thematik der Krisenbewältigung bestimmen statt der es bedrohenden Risiken und Gefahren. In dieser Perspektive bildet das unerwünschte Ereignis den Hintergrund, in den Vordergrund treten Aspekte von Robustheit in einem engeren fachspezifischen Kontext und Resilienz in einem breiteren, sich derzeit entwickelnden Horizont. So finden sich Themen zur Robustheit vor allem in der Fachliteratur (z.B. zur Softwareentwicklung), wobei die Aufmerksamkeit den Schwachstellen (Anfälligkeiten, Verletzbarkeiten) des Systems im Hinblick auf identifizierbare Fehler oder Störungen gilt. Die Interaktion der Beteiligten ist entsprechend geprägt durch Aufgabenbeschreibung und Problemlösungen auf der Basis des domänenspezifischen Fachwissens.

Das Thema Resilienz hat viel zu tun mit Kommunikation. Entfaltet im Sinne aktiver Widerständigkeit, Regenerationsfähigkeit, Einfallsreichtum, Fähigkeiten zur Identifikation von Ressourcen und Handlungsalternativen, zu Kooperation und Vertrauensbildung ist es ein Thema, das durch die Disziplinen wandert (s.o. 3.5). Die Entwicklung ist gegenwärtig offen und tendiert zu einer zunehmenden „Interdisziplinierung“ (vgl. Weber 2010), in der Sicherheitsfragen in der Integration mit anderen Diskursen neu gestellt werden (z.B. Gesundheit, Nachhaltigkeit, Frieden; vgl. Parodi et al. 2010).

Zusammenfassung: Die Kommunikationskultur der Robustheit und Resilienz fokussiert auf die Schwächen bzw. Stärken der (biologischen, sozialen, technischen) Systeme und zielt dabei auf die Verringerung der Schwächen und die Erhöhung der Stärken. Die Handlungen der Interaktion sind einerseits eingebunden in fachspezifische Problemlösungsverfahren, andererseits in offene interdisziplinäre Diskurse.

Zum elaborierten Begriffsfeld gehören u.a. *Robustheit: Anfälligkeit, Empfindlichkeit*, *Verletzlichkeit, Verletzbarkeit, Vulnerabilität*; *Widerstandsfähigkeit, Redundanzen*; *Resilienz*: *Widerständigkeit, schnelle Regenerations- und Reaktionsfähigkeit, Ressourcenkompetenz, Einfallsreichtum, Kommunikations- und Kooperationsfähigkeit.*

5. Fazit

In der Analyse der Sicherheitskommunikation wird sichtbar, welche Phänomene in einer Kultur als sicherheitsrelevant betrachtet, wie sie strukturiert

und bewertet werden. Die unterschiedlichen Ausprägungen im Kontext der Kommunikation lassen sich wiederum als typische Muster einer Kommunikationskultur beschreiben. Wir haben vier Typen unter dem Aspekt des kommunikativen Umgangs mit dem Thema Sicherheit unterschieden:

1. Sicherheit ist kein Thema, weil sie nicht als Unsicherheit verstanden wird;
2. Sicherheit wird unter dem abstrakten Aspekt Risiko in der öffentlichen Debatte kontrovers behandelt (Akzeptanz bzw. Nicht-Akzeptanz);
3. Sicherheit gilt als Problem der Praxis mit konkreten Maßnahmen mit stillschweigender Akzeptanz, weil das Ergebnis erwünscht ist bzw. mit Ablehnung, weil Konflikte mit anderen Werten entstehen;
4. das Thema Sicherheit im Sinne der Reaktion auf Einwirkungen aus der Außenwelt verschiebt sich in Richtung der Systeme selbst, die aus eigener Kraft heraus nach außen wirken. Letzteres verlangt stärkere Integration erweiterter Kontexte. Daraus ergeben sich interdisziplinäre Themenfelder, die sich aktuell in der Entwicklung befinden.

Kommunikationskulturen können generell im Hinblick auf thematische oder institutionelle Zuordnungen differenziert werden (eine mediale Differenzierung ist hier untergeordnet). Unter thematischen Gesichtspunkten bilden sie eine Komponente der in einer Gesellschaft etablierten Sicherheitskulturen (vgl. Banse 2011, S. 209). Unter institutionellen Aspekten sind sie eingebettet in übergeordnete Organisationsstrukturen. In diesem Sinne unterscheidet Lucie Hribal Unternehmenskulturen danach, inwieweit sie durch proaktive und transparente Kommunikationskulturen, z.B. im Hinblick auf die Themen Risiko und Sicherheit, geprägt sind (vgl. Hribal 1999, S. 477). Themen, Kulturen und Kommunikation bilden dabei einen Zusammenhang, in dem Realsituationen und Kommunikationssituationen systematisch aufeinander beziehbar sind. In diesem Beitrag stand die Richtung von der Realsituation zur Kommunikationssituation im Fokus, der Blick in umgekehrter Richtung ist ein Desiderat für die Forschung (vgl. Felder 2013).

Literatur

Andrejevic, M. (2011): Securitainment in the Post-9/11 Era. In: Continuum. Journal of Media & Cultural Studies, Vol. 25, No. 2, pp. 165-175

Banse, G. (Hg.) (1996): Risikoforschung zwischen Disziplinarität und Interdisziplinarität. Von der Illusion der Sicherheit zum Umgang mit Unsicherheit. Berlin

Banse, G. (2010): Techniksicherheit und Sicherheitskulturen. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 185-205

Banse, G. (2011): Im Fokus der Sicherheitsforschung. In: Banse, G.; Krebs, I. (Hg.): Kulturelle Diversität und Neue Medien. Entwicklungen – Interdependenzen – Resonanzen. Berlin, S. 207-227

Bechmann, G.; Stehr, N. (2000): Risikokommunikation und die Risiken der Kommunikation wissenschaftlichen Wissens. Zum gesellschaftlichen Umgang mit Nichtwissen. In: GAIA – Ecological Perspectives for Science and Society, Jg. 9, H. 2, S. 113-121

Beck, U. (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main

Beck, U. (2007): Weltrisikogesellschaft. Frankfurt am Main

Becker, U. (1993): Risiko ist ein Konstrukt. München

Beyerer, J.; Geisler, J.; Dahlem, A.; Winter, P. (2010): Sicherheit: Systemanalyse und –design. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 39-72

Bidlo, O.; Englert, C. (2009): Securitainmant. Mediale Inszenierung von Innerer Sicherheit. In: MEDIENwissenschaft, H. 3, S. 244-260

Bohle, H.-G. (2008): Leben mit Risiko – Resilience als neues Paradigma für die Risikowelten von morgen. In: Felgentreff, C.; Glade, T. (Hg.): Naturrisiken und Sozialkatastrophen. Berlin, S. 435-442

Bonfadelli, H. (2012): Fokus Grüne Gentechnik: Analyse des medienvermittelten Diskurses. In: Weitze, M.-D.; Pühler, A. (Hg.): Biotechnologie-Kommunikation. Kontroversen, Analysen, Aktivitäten. München (acatech), S. 205-252

Bonß, W. (1995): Vom Risiko. Unsicherheit und Ungewissheit in der Moderne. Hamburg.

Bonß, W. (2010): (Un-)Sicherheit als Problem der Moderne. In: Münkler, H.; Bohlender, M.; Meurer, S. (Hg.): Handeln unter Risiko. Bielefeld, S. 33-63

Boysen, M. (2012): Grüne Gentechnik: Konflikte mit Fortsetzung bei der synthetischen Biologie? In: Weitze, M.-D.; Pühler, A. (Hg.): Biotechnologie-Kommunikation. Kontroversen, Analysen, Aktivitäten. München (acatech), S. 15-64

Brand, F. S.; Jax, K. (2007): Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Objekt. In: Ecology and Society, Jg. 12 (1), H. 23. URL: http://www. ecologyandsociety.org/vol12/iss1(art23) [20.04.2013]

Campo, M. a (2001): PC-Sicherheit. Bonn

Dobler, M. (2004): Risikoberichterstattung. Eine ökonomische Analyse. Frankfurt am Main

Dombrowsky, W. R. (2005): Warnen und Reagieren – Ist der Mensch von technischen Systemen überfordert. In: Stiftung Umwelt und Schadenvorsorge (Hg.): Naturgefahren und Kommunikation. Sonderheft Nr. 3. München, S. 7-8

DUDEN (2002): Das Bedeutungswörterbuch. Wortschatz und Wortbildung. Bd. 10. Mannheim. –
URL: http://www.duden.de/rechtschreibung/Sicherheit [20.04.2013]

Dutke, S. (1994): Mentale Modelle: Konstrukte des Wissens und Verstehens. Kognitionspsychologische Grundlagen für die Software-Ergonomie. Göttingen

Folke, K. (2006): Resilience: The Emergence of a Perspective for Social-ecological Systems Analyses. In: Global Environmental Change, Vol. 16, pp. 253-267

Fratzscher, W. (2011): Zu Risiken und Nebenwirkungen lesen Sie den Sicherheitsbericht oder fragen Sie… In: Banse, G.; Reher, E.-O. (2011): Ambivalenzen von Technologien – Chancen, Gefahren, Missbrauch. Berlin, S. 131-141 (Sitzungsberichte der Leibniz-Sozietät der Wissenschaften, Bd. 112)

Gabriel, T. (2005): Resilienz – Kritik und Perspektiven. In: Zeitschrift für Pädagogik, Jg. 51, H. 2, S. 207-217

Giebel, D. (2012): Integrierte Sicherheitskommunikation. Zur Herausbildung von Unsicherheitsbewältigungskompetenzen durch und in Sicherheitskommunikation. Berlin

Gill, B. (2012): Utilitaristische Motive der Kritik – Warum die europäischen Bauern mehrheitlich nicht so begeistert von der Gentechnik sind. In: Weitze, M.-D.; Pühler, A. (Hg.): Biotechnologie-Kommunikation. Kontroversen, Analysen, Aktivitäten. München (acatech), S. 65-67

Grunwald, A. (2005): Zur Rolle von Akzeptanz und Akzeptabilität von Technik bei der Bewältigung von Technikkonflikten. In: Technikfolgenabschätzung – Theorie und Praxis, Jg. 14, H. 3, S. 54-60

Grice, H. P. (1975): Logic and Conversation. In: Cole, P.; Morgan, J. L. (eds.): Syntax and Semantics 3: Speech Acts. New York, pp. 41-58

Hansen, K. P. ([4]2011): Kultur und Kulturwissenschaft. Tübingen

Hennig, J.; Tjarks-Sobhani, M. (Hg.) (1999): Verständlichkeit und Nutzungsfreundlichkeit von Technischer Dokumentation. Lübeck

Hribal, L. (1999): Public Relations-Kultur und Risikokommunikation. Konstanz

Jacob, K. (1991): Maschine, mentales Modell, Metapher. Studien zur Semantik und Geschichte der Techniksprache. Tübingen

Johnson-Laird, P. (1983): Mental Models. Towards a Cognitive Science of Language, Inference, and Consciousness. Cambridge, MA

Juhl, D. (2002): Technische Dokumentation. Praktische Anleitungen und Beispiele. Berlin

Kaminski, A. (2010): Technik als Erwartung. Grundzüge einer allgemeinen Technikphilosophie. Bielefeld

Krüger, J.; Ruß-Mohl, S. (Hg.) (1991): Risikokommunikation. Technikakzeptanz, Medien und Kommunikationsrisiken. Berlin

Lange, H.-J.; Endreß, C.; Wendekamm, M. (Hg.) (2013): Sicherheitskultur. Interdisziplinäre Betrachtung einer mehrdimensionalen Begrifflichkeit. Wiesbaden

Lazarding, J. (2006): Die Maschine als Spektakel. Funktion und Admiration im Maschinendenken des 17. Jahrhunderts. In: Schramm, H.; Scharte, L.; Lazardig, J. (Hg.): Instrumente in Wissenschaft und Kunst. Zur Architektonik kultureller Grenzen im 17. Jahrhundert. Berlin, S. 167-193

Liebert, W.-A. (2004): Diskursdynamik in der Risikokommunikation. Eine diskurslinguistische Untersuchung der Trierer Luftschadstoff-Debatte 1974-2001. In: Deutsche Sprache, Jg. 32, S. 137-161

Luhmann, N. (1991): Soziologie des Risikos. Berlin

Maier-Rabler, U.; Latzer, M. (Hg.) (2001): Kommunikationskulturen zwischen Kontinuität und Wandel. Universelle Netzwerke für die Zivilgesellschaft. Konstanz

MPG – Max-Planck-Gesellschaft (Hg.) (2009): Katalog zu Expedition Zukunft. Darmstadt. – URL: http://www.expedition-zukunft.org [20.04.2013]

Metz, K. H. (2006): Ursprünge der Zukunft. Die Geschichte der Technik in der westlichen Zivilisation. Paderborn

Münkler, H.; Bohlender, M.; Meurer, S. (Hg.) (2009): Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert. Bielefeld

Münkler, H. (2010): Sicherheit und Freiheit. Eine irreführende Oppositionssemantik der politischen Sprache. In: Münkler, H.; Bohlender, M.; Meurer, S. (Hg.): Handeln unter Risiko. Bielefeld, S. 13-32

Neubert, C.; Schabacher, G. (Hg.) (2013): Verkehrsgeschichte und Kulturwissenschaft. Analysen an der Schnittstelle von Technik, Kultur und Medien. Bielefeld

Obermeier, O. P. (1999): Die Kunst der Risikokommunikation. München

Parodi, O.; Banse, G.; Schaffer, A. (Hg.) (2010): Wechselspiele: Kultur und Nachhaltigkeit. Annäherungen an ein Spannungsfeld. Berlin

Regenfuß, T.; Viehweg, K. (2010): Sicherheits- und Risikoterminologie im Spannungsfeld von Technik und Recht. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 131-144

Rifkin, J. (2003): Das biotechnische Zeitalter. Die Geschäfte mit der Gentechnik. München

Renn, O. (2010): Sicherheit, Risiko und Vertrauen. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 163-183

Ropohl, G. (2009): Allgemeine Technologie. Eine Systemtheorie der Technik. 3. Aufl. Karlsruhe

Rothkegel, A. (2010a): Technikkommunikation. Produkte, Texte, Bilder. Konstanz (UTB 3214)

Rothkegel, A. (2010b): Sicherheitsmodelle und Kommunikationsrisiko. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (atatech), S. 207-220

Rothkegel, A. (2011): Sicherheit durch Kommunikation: ein linguistischer Forschungsansatz. In: Banse, G.; Krebs, I. (Hg.): Kulturelle Diversität und neue Medien. Entwicklungen – Interdependenzen – Resonanzen. Berlin, S. 269-284

Schirmer, W. (2008): Bedrohungskommunikation. Eine gesellschaftstheoretische Studie zu Sicherheit und Unsicherheit. Wiesbaden

Schulz, G. (1992): Die Erlebnisgesellschaft. Kultursoziologie der Gegenwart. Frankfurt am Main

Schwarz, M. (2008): Einführung in die kognitive Linguistik. 3. Aufl. Tübingen

Stieniczka, N. (2006): Das „narrensichere“ Auto. Die Entwicklung passiver Sicherheitstechnik in der Bundesrepublik Deutschland. Darmstadt

Thoma, K.; Drees, B.; Leismann, T. (2010): Zukunfstechnologien in der Sicherheitsforschung. In: Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.): Sicherheitsforschung – Chancen und Perspektiven. München (acatech), S. 13-37

Torgersen, H.; Schmidt, M. (2012): Perspektiven der Kommunikation für die synthetische Biologie. In: Weitze, M.-D.; Pühler, A. (Hg.): Biotechnologie-Kommunikation. Kontroversen, Analysen, Aktivitäten. München (acatech), S. 113-154

Trischler, H.; Weitze, M.-D. (2006): Kontroversen zwischen Wissenschaft und Öffentlichkeit. Zum Stand der Diskussion. In: Liebert, W.-A.; Weitze, M.-D. (Hg.): Kontroversen als Schlüssel zur Wissenschaft. Wissenskulturen in sprachlicher Interaktion. Bielefeld, S. 57-80

Weber, H. (2006): Technik für den Taumel. Erlebniswelten der Berliner Unterhaltungskultur von 1880 bis 1910. In: Poser, S.; Hoppe, J.; Lüke, B. (Hg.): Spiel mit Technik. Katalog zur Ausstellung im Deutschen Technikmuseum Berlin. Leipzig, S. 36-41

Weber, J. (Hg.) (2010): Interdisziplinierung? Zum Wissenstransfer zwischen den Geistes-, Sozial- und Technowissenschaften. Bielefeld

Weingart, P. (2005): Die Wissenschaft der Öffentlichkeit. Essays zum Verhältnis von Wissenschaft, Medien und Öffentlichkeit. Weilerswist

Weitze, M.-D.; Pühler, A. (Hg.) (2012): Biotechnologie-Kommunikation. Kontroversen, Analysen, Aktivitäten. München (acatech)

Winzer, P.; Schnieder, E.; Bach, F.-W. (Hg.) (2010): Sicherheitsforschung – Chancen und Perspektiven. München (acatech)

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 145–160*

Martin Endreß, Benjamin Rampp

Vertrauen in der Sicherheitsgesellschaft

1. Einleitung

In einer als Sicherheitsgesellschaft konzipierten, spätmodernen Gesellschaftskonstellation sind die gesellschaftlichen (Neben-)Folgen und paradoxen Effekte von sozialer Kontrolle bzw. Regierung und damit zusammenhängend der Herstellung von Sicherheit vielfältig.[1] Im Nachfolgenden werden die Folgen für ein spezifisches, für Vergesellschaftungsprozesse zentrales Phänomen in den Blick genommen: dem des Vertrauens. Einführend wird zunächst erläutert, was mit dem Begriff einer (spätmodernen) Sicherheitsgesellschaft gemeint ist. Dazu werden aktuelle Phänomene gesellschaftlicher Unsicherheit und Ungewissheit skizziert, der Wandel des Sicherheitsverständnisses adressiert und auf die zentrale Rolle des Konzepts des Risikos eingegangen. Daran anschließend werden in historisch-systematischer Absicht zwei Idealtypen von Sicherheitspraktiken unterschieden, um den historischen Wandel von Formen und Modi der Sicherheitsproduktion im Zuge der Entwicklung von Gegenwartsgesellschaften veranschaulichen zu können. Die Unterscheidung von Modi des Vertrauens eröffnet dann die Chance, die jeweiligen Effekte der unterschiedenen Idealtypen von Sicherheitspraktiken auf je spezifische Vertrauensmodi herauszuarbeiten.

2. Spätmoderne Gesellschafskonstellationen und das Konzept der Sicherheitsgesellschaft

Die Herausforderungen für Gegenwartsgesellschaften insbesondere des sogenannten westlichen Typus hinsichtlich von Fragen der Sicherheit und der gesamtgesellschaftlichen Etablierung und Stabilisierung grundlegender Gewissheiten u.a. für alltägliche Handlungsvollzüge haben sich in den vergangenen

1 Vgl. generell zur aktuellen Relevanz und zum systematischen Zuschnitt des Konzepts der Nebenfolgen für die Soziologie in historisch-systematischer Perspektive Endreß 2010c.

Jahren grundlegend gewandelt. Diese Befunde werden im Nachfolgenden skizziert und konzeptionell auf ein Verständnis der Gegenwartsgesellschaft als einer Sicherheitsgesellschaft zugeschnitten werden.

2.1 Spätmoderne und Flexibilisierung

Eine der weitreichendsten und grundlegendsten gesellschaftlichen Entwicklungen der jüngeren Vergangenheit betrifft Neoliberalisierungsprozesse seit spätestens den 1970er Jahren. Diese betreffen insbesondere klassische wohlfahrtstaatliche Arrangements, d.h. das Zurücktreten staatlich garantierter Sicherungssysteme zugunsten privater Vorsorge- und Sicherungseinrichtungen. Diese Prozesse werden flankiert von einer Flexibilisierung sozialer Strukturen und individueller Biographien und sind im Kontext der zunehmenden Bedeutung einer Rationalität des Liberalismus zu verorten (vgl. Foucault 2006b; Garland 2008, S. 334ff.; Krasmann 2003, S. 175ff.). Die gesellschaftstheoretischen Angebote bspw. der „Risikogesellschaft", der „Zweiten Moderne" bzw. der „Reflexiven Modernisierung" (vgl. Beck 1986, 1993; Beck et al. 1996) – mit ihrem Augenmerk auf Nebenfolgen (vgl. Böschen et al. 2006) – oder auch der „Erlebnisgesellschaft" (vgl. Schulze 1992), des „flexiblen Selbst" und der „Kultur des neuen Kapitalismus" (vgl. Sennett 1998, 2007) etc. haben darauf reagiert und versuchen, das Phänomen analytisch zu fassen.

Die Flexibilität und Multioptionalität (vgl. Gross 1994) sozialer Konstellationen und Verhältnisse, und damit ebenso von traditionellen, habitualisierten und sedimentierten Regeln des sozialen Verkehrs und sozialer Normalitätsvorstellungen sowie von individuellen Biographien und Lebensstilen haben zu einer zumindest dreifachen Verunsicherung und zu neuen bzw. forcierten Ungewissheiten geführt. Dies sind (1) die neuen Ungewissheiten und Unsicherheiten von Erwerbsbiographien und – in deren Gefolge – von allgemeinen aktuellen Lebensumständen wie zukünftigen Versorgungsoptionen weiter Bevölkerungsteile; damit verbunden (2) eine offenkundige Fragilisierung sozialer Bindungen und Zugehörigkeiten (vgl. Baudrillard 1983; Bauman 2003) und schließlich (3) die individualisierte Zumutung, aktiv einen gesellschaftlichen Ort für sich selbst zu suchen sowie eine persönliche Identität im Modus eines „Unternehmers seiner selbst" (Foucault 2006b, S. 314; vgl. Bröckling 2007) zu produzieren. Auf diese Weise unterlaufen Flexibilisierungsprozesse vormals routinisierte und als selbstverständlich angenommene und etablierte Modi der Subjektivierung, führen zu einer forcierten Gewichtung der Suche nach Sicherheit(en) als zentralem Fokus individuellen wie sozialen (gesellschaftlichen) Lebens und zwingen Individu-

en in einen kontinuierlichen Prozess der Selbstproblematisierung unter den Vorzeichen von Leistungszumutungen und Verantwortungszurechnungen: Selbstvergewisserung wird zur unabschließbaren Aufgabe.

2.2 Wandel des Sicherheitsverständnisses

Die zuvor skizzierten Befunde betreffen Fragen von Vergesellschaftungsprozessen insgesamt und prägen damit den Hintergrund, vor dem Sicherheitspraktiken – die sich v.a. auf Sicherheit im Sinne von „security", also auf „Angriffssicherheit", beziehen – im Nachfolgenden analysiert werden.

Parallel zu den Prozessen der Neoliberalisierung erfuhr das Konzept der Sicherheit, das in politischer wie wissenschaftlicher Hinsicht bis in die 1950/60er Jahre als vornehmlich den militärischen Bereich staatlicher Politik betreffender Begriff zur Verwendung kam, eine deutliche Ausweitung. Die Ausweitung des Konzeptes kann in Anschluss an Roland Paris (2001) in der horizontalen Dimension des Sachbezuges als „broadening", in der vertikalen Dimension der Analyseebene als „deepening" bezeichnet werden. Christopher Daase (2010a) beschreibt die damit angedeutete Erweiterung des Sicherheitsbegriffs – analytisch verfeinert – in vier Dimensionen: in der Raumdimension (von einem nationalen hin zu einem regionalen, internationalen und schließlich globalen Fokus), der Referenzdimension (vom Staat zur Gesellschaft und schließlich zum Individuum), der Sachdimension (von einer Beschäftigung mit vornehmlich militärischen Herausforderungen zur Fokussierung auch auf ökonomische, ökologische und schließlich humanitäre Sachverhalte) und schließlich der Gefahrendimension (vom Bedrohungsbegriff zur Verwundbarkeit und schließlich zum Risiko). Die Erweiterung des Sicherheitsbegriffes in mehreren Dimensionen führt also zu einer zunehmenden Ausweitung des Anwendungsfeldes des Konzepts der Sicherheit und – damit verknüpft – zu seiner fortschreitenden begrifflichen Unschärfe, welche jedoch zugleich elementarer Bestandteil der breiten Verwendungsweise ist.[2]

2.3 Risiko und Proaktivität

Im Rahmen der Erweiterung des Sicherheitsbegriffs ist vor allem die Fokussierung von Risiken von zentraler Bedeutung – sowohl für Formen der Ver-

2 Vgl. hierzu die Ansätze der Securitization-Forschung, die Sicherheit als soziale Konstruktion konzipieren und analysieren, welche Folgen die „Versicherheitlichung" vormals nicht mit der Logik der Sicherheit verknüpfter Felder zeitigt (vgl. Balzacq 2011; Wæver 1995).

gesellschaftung im Allgemeinen als auch für Sicherheitspraktiken im Besonderen.

Die Orientierung am Konzept des Risikos reflektiert die Fokussierung neuer Gefährdungen von Sicherheit. Diese werden als Verschiebungen von relativ klar umrissenen, beobachtbaren und abschätzbaren Bedrohungen hin zu eher diffus bleibenden Risiken wahrgenommen (vgl. Daase 2002, S. 14ff.) und gedeutet, die (1) vor allem die Frage der Eintrittswahrscheinlichkeit aufwerfen, also die Frage des „wann", nicht die des „ob" – und zwar auch dann, wenn die jeweiligen Wahrscheinlichkeiten sehr gering sind; die sich sodann (2) mit kaum identifizierbaren Akteuren der Risikoerzeugung verbinden, und die schließlich (3) in wechselseitiger Abhängigkeit stehen zu den von Sicherheitsakteuren vollzogenen eigenen Handlungen und Gegen-Reaktionen. Im Fokus steht also die Wahrscheinlichkeit zukünftiger Schädigungen, die durch gegenwärtiges Handeln (sowohl von potenziellen Gefährdern bestimmter Güter als auch von Sicherheitsakteuren selbst) ausgelöst oder forciert werden (und insofern ist der Risikobegriff auch von dem der Gefahr zu unterscheiden; vgl. Evers/Nowotny 1987, S. 34; Luhmann 1991, S. 25). Man kann das systematisch als Konsequenz der neuen gesellschaftlichen Aufmerksamkeit auf Nebenfolgen und damit zugleich auf die paradoxen Effekte von Sicherungs- und Schutzmaßnahmen deuten.

Die räumliche, zeitliche und soziale Allgegenwärtigkeit von Risiken und eines Risikobewusstseins, das Sicherheitspolitik konstruktiv aufzunehmen hat, verändert den Charakter dieser von einer primär reaktiven zu einer vermehrt (und ggf. dominant) proaktiven Handlungslogik (vgl. Daase 2002, S. 18ff.). Dieser Logik folgend müssen Sicherheitspraktiken vorgreifend auf unterstellte Wahrscheinlichkeiten ausgerichtet sein und nicht erst dann aktiviert werden, wenn konkrete Gefahren absehbar sind, sondern bereits zuvor die Wahrscheinlichkeit des potenziellen Eintritts eines Schadensfalls ebenso wie die potenziell eintretende Schadenshöhe zu mindern versuchen.[3] Sicherheitspraktiken sind in diesem Sinne also strukturell darauf angelegt, Risiken a priori zu begegnen, also bevor diese realisiert werden, und stehen damit vor dem Problem, selbst ein riskantes Handeln mit potenziellen Nebenfolgen darzustellen.[4]

---

3 Insofern ist zwischen unterschiedlichen Formen der Proaktivität zu unterscheiden (vgl. Daase 2002, S. 18): Prävention, die vorbeugend die Eintrittswahrscheinlichkeit fokussiert, und Präkaution, die vorsorgend die (eventuelle) Schadenshöhe in den Blick nimmt.

4 Man kann darin eine Forcierung der „Entdeckung der Gestaltbarkeit von Gesellschaft" identifizieren (vgl. Evers/Nowotny 1987).

2.4 Sicherheitsgesellschaft

Vor diesem Hintergrund neuer Unsicherheiten, der Erweiterung des Sicherheitsbegriffes und der Einnahme einer v.a. am Risiko orientierten Perspektive wird Sicherheit zu einer zentralen Wertidee in der Gegenwartsgesellschaft, wie Franz-Xaver Kaufmann schon zu Beginn der 1970er Jahre – wenn auch mit primärem Blick auf sozialpolitische Problemstellungen – herausgearbeitet hat (vgl. Kaufmann 1973). Dabei ersetzt das Konzept der Sicherheit das des Friedens als zentralem Wertbegriff, wie auch Daase mit Blick auf gegenwärtige Politikstrategien formuliert: „Heute ist ‚Sicherheit' der Goldstandard nationaler und internationaler Politik, und vom Frieden wird fast nur noch in politischen Sonntagsreden gesprochen" (Daase 2010b, S. 9). Insofern kann die Gegenwartsgesellschaft als Sicherheitsgesellschaft bezeichnet werden (vgl. Foucault 2006; Groenemeyer 2010; Legnaro 1997; Singelnstein/Stolle 2012), die gerade durch die strukturelle Ambivalenz zwischen grundsätzlicher Verunsicherung und permanentem Streben nach Sicherheit zu charakterisieren ist.

3. Zwei Idealtypen von Sicherheitspraktiken

In Reaktion auf das veränderte Verständnis von Sicherheit und die Fokussierung neuer Herausforderungen haben sich ebenso die Modi sozialer Kontrolle und die Praktiken der Sicherheitsproduktion gewandelt.

Entsprechend lassen sich in historisch-systematischer Absicht zwei Formen von Sicherheitspraktiken – idealtypisch – unterscheiden: der exkludierend-disziplinierende Idealtypus auf der einen und der liberal-inkludierende Idealtypus auf der anderen Seite. Diese Unterscheidung schreibt sich selbstverständlich von Foucaults Governmentalitätsstudien her (vgl. Foucault 2006a, 2006b), erhält ihre Impulse aber ebenso aus jüngeren Arbeiten zu den Formen sozialer Kontrolle in Gegenwartsgesellschaften, wie sie sich in den Konzepten der „Kontrollgesellschaft" (vgl. Deleuze 1993; Garland 2008) oder der „Sicherheitsgesellschaft" (s.o.; vgl. Singelnstein/Stolle 2012, S. 74ff.) finden.

3.1 Exkludierend-disziplinierender Idealtypus von Sicherheitspraktiken

Für den exkludierend-disziplinierenden Typus der Sicherheitsproduktion können zwei Varianten von Sicherheitspraktiken unterschieden werden: einerseits Praktiken des Ausschließens bzw. der Exklusion, andererseits Prak-

tiken des Kontrollierens und des Überwachens (vgl. Singelnstein/Stolle 2012, S. 79ff.). In der von Foucault entwickelten Analytik werden damit die souverän-juridische und die disziplinarische Form von Macht angesprochen, die Foucault v.a. in „Überwachen und Strafen" thematisiert (vgl. Foucault 1977).

Praktiken des Ausschließens/der Exklusion (und damit zugleich auch des Weg- bzw. Einsperrens) wirken unmittelbar bzw. direkt und schließen die Ausübung von direkten Zwangsmitteln dort ein, wo liberale Formen der Sicherheit als nicht ausreichend begriffen werden oder aber – aus welchen Gründen auch immer – nicht zur Anwendung kommen. Diese Sicherheitspraktiken sind im Kern zugeschnitten auf eine Logik des Ausnahmezustandes (vgl. Agamben 2004; Schmitt 1993), sind also als souveräne Praktiken zu verstehen, die die Verfügbarkeit einer breiten Palette möglicher Maßnahmen von Stigmatisierungsprozessen bis hin zu gewaltförmiger körperlicher Ausgrenzung nach sich zieht und impliziert. Beispiele solcher Maßnahmen können Gefängnisse, Lager oder aber – sozusagen final – die Todesstrafe sein. Über das Verfahren der Ausgrenzung werden Risikofaktoren und Risikogruppen nicht nur systematischer Kontrolle unterzogen, sondern im Kern als solche gerade erst konstituiert bzw. generiert. Praktiken wie diese markieren die veränderten und die sich (offenkundig weiter) verändernden Grenzen freier gesellschaftlicher Räume.

Praktiken des Kontrollierens und des Überwachens beziehen sich daneben auf das Phänomen sowie die Diskussionen um die Typik des Panoptismus und repräsentieren entsprechend eine zwischen den zwangsförmigen und den liberalen Praktiken angesiedelte mittlere Form von Sicherheitspraktiken. Sie zielen im Effekt nicht ausschließlich und primär auf Formen des Strafens, sondern auch auf Formen der Selbstführung. Sie stehen damit in Kontinuität zu klassischen soziologischen Analysen moderner Gesellschaften als Disziplinargesellschaften bei Max Weber und Norbert Elias. Im Unterschied jedoch zu liberal-inkludierenden Formen sind diese Praktiken des Kontrollierens zumindest durch den direkten Bezug auf Möglichkeiten des Strafens und weitergehende Zwangsmaßnahmen charakterisiert. Besonders anschaulich wird das bspw. beim Gebrauch von Überwachungskameras. Praktiken des Kontrollierens und des Überwachens sind hier, im Kontrast zu liberal-inkludierenden Formen der Sicherheitsproduktion, verknüpft mit signifikant ausgeprägten und explizierten Normalitätserwartungen an das Verhalten und sie sind darüber hinaus vor allem bezogen auf eindeutig identifizierbare Räume; wobei der Zugang zu diesen Räumen typischerweise ebenso unter Kontrolle gestellt ist.

3.2 Liberal-inkludierender Idealtypus von Sicherheitspraktiken

Liberal-inkludierende Typen der Sicherheitsproduktion verfolgen dagegen Formen indirekter, „zurückhaltend-distanzierter", subtiler Kontrolle, die vorrangig über Anreizsysteme funktionieren (vgl. Singelnstein/Stolle 2012, S. 74ff.). Im Rahmen dieses Typus werden alle Verhaltensweisen etc., die sich im Horizont bestimmter Normalitätsvorstellungen bewegen – und somit ein bestimmtes Maß an Abweichung nicht überschreiten –, einem Modus der Sicherheitsproduktion im Sinne einer „Verwaltung des empirisch Normalen" (ebd, S. 61; vgl. Foucault 2006a, S. 87ff.) ohne die Anwendung direkter Zwangsmaßnahmen unterworfen. Entsprechend schließt dieser Idealtypus an liberale Regierungsformen an, wie sie Foucault in seinen Vorlesungen zur Gouvernementalität und seinen Arbeiten zur Thematik der Subjektivierung angesprochen hat (vgl. z.B. Foucault 2006a, 2006b, 2009).

Ganz im Gegenteil ist im Rahmen dieses Typus' zu beobachten, wie soziale Strukturen und individuelle Biographien bzw. Lebensentwürfe über die Implementierung eines strukturellen Zwangs zur Selbstverantwortung dem Gebot ihrer eigenen Sicherheit formiert werden. Dieses Ethos der Responsibilisierung greift auf den Individualtätstypus eines „Unternehmers seiner selbst" (s.o.) zurück und kann deshalb wohl adäquat als Form der Etablierung eines Modus der Selbstführung beschrieben werden. Die liberal-inkludierenden Formen gewinnen ihre Steuerungs- oder Regierungswirkung auf der Basis eines Angstszenarios, das sich auch durch bzw. über Formen sozialer Schließung und Ausschließung speist, also von diesen unterfüttert und somit getragen wird.[5] Diese Praktiken sind aber ihrerseits gerade nicht auf extreme Situationen bzw. Konstellationen der Unsicherheit und des Schreckens bezogen, sondern umgekehrt auf alltägliche Lebenssituationen und Lebensumstände – und sie erlangen gerade durch diesen Bezug ihre herausragende Wirkung. Es sind also nicht mehr die mehr oder weniger markanten sozialen Abweichungen, auf die das Augenmerk sozialer Kontrolle gerichtet wird, sondern es sind die vermeintlich kleinen, die so unscheinbaren Auffälligkeiten, Merkwürdigkeiten (Anomalien), das (vermeintliche) Nicht-Beachten bzw. Nicht-mehr-Einhalten von als selbstverständlich angenommenen Regeln sozialen Verkehrs, die (vermeintliche) Aufkündigung bzw. das Abwei-

5 D.h. die Angst vor dem Nicht-mehr-dazu-zu-gehören. Im Sinne Foucaults geht es also – in Verbindung mit biopolitischen Rationalitäten – auch um einen „Staatsrassismus" (vgl. Foucault 1999, S. 74ff.; Lemke 1997, S. 224ff.) und die Angst vor dem Abstieg in die „gefährlichen Klassen" (vgl. Garland 2008, S. 281ff.; Lemke 1997, S. 228ff.; Singelnstein/Stolle 2012, S. 34ff., 45f.; Wacquant 2009).

chen von unterstellten Einverständnissen, auf die die soziale Aufmerksamkeit gerichtet wird. Dieses eminente Absenken der Sensibilitätsschwelle für sogenannte Auffälligkeiten verschiebt entsprechend das Koordinatensystem sozialer Relevanzen: nicht mehr um direkten, eklatanten Normverstoß geht es, sondern um die Achtsamkeit auf Andersartigkeit, auf Abweichungen und abweichendes Verhalten jedweder Art und Form. Zugespitzt formuliert haben wir es mit einer Verschiebung der Aufmerksamkeitsausrichtung von den Anomien zu den Anomalien zu tun. Entsprechend richtet sich die *attention à la vie* auf den gesamten Kosmos individueller Lebensführung: vom Lebensstil über habituelle Ausprägungen bis hin zu religiösen Bekenntnissen und Konsumpraktiken. Die Potenzialität des Verdachts kennt eben *per definitionem* keine Grenzen.

Mit Foucault lässt sich deshalb durchaus von einem neoliberalen Sicherheitsdispositiv sprechen (vgl. Foucault 2006a, 2006b). Mit Blick auf die soziologische Tradition lässt sich aber ebenso auf Norbert Elias' Hinweise zum historischen Wandel von Formen des „Fremdzwanges" hin zum Typus des internalisierten „Selbstzwanges" im Rahmen seiner Analyse des abendländischen Zivilisationsprozesses verweisen (vgl. Elias 1969).

Zusammenfassend lassen sich in idealtypischer Absicht also zwei Typen von Sicherheitspraktiken relativ klar voneinander unterscheiden: Der exkludierend-disziplinierende Typus lässt sich charakterisieren als ausschließend, direkt, sichtbar und normativ aufgeladen. Er arbeitet mit Zwang und extern induzierten Regierungsformen, die auf den Körper der Regierten mittels negativer Stigmatisierungen (vgl. Neckel/Sutterlüty 2005) abstellen und solchermaßen exklusive, eindeutig regulierte Räume erzeugen.

Im Unterschied dazu basiert der liberal-inkludierende Typus auf Mechanismen der Produktion einer sozialen Gesamtheit, eines „totalen" sozialen Körpers,[6] mittels indirekter und unsichtbarer Instrumente. Hier geht es um ein „Management des empirisch Normalen", um die Etablierung interner Kontrollmechanismen im Sinne eines Subjektivierungsprozesses, die Etablierung einer Selbstzurechnungskultur, d.h. die Einsetzung des selbstverantwortlichen, responsibilisierten Subjekts – und zwar nicht mittels sozialer Stigmatisierungsprozesse und der Schaffung exklusiver Räume, sondern umgekehrt im Sinne gesellschaftlicher Normalitätsvorstellungen und -erwartun-

6 Man denke an Foucaults „Omnes et singulatim" in Bezug auf die Aspekte der Pastoralmacht und der Biopolitik: Regierung bezieht sich auf jeden Einzelnen, aber im Kontext eines Gesellschaftskörpers (vgl. Foucault 2005).

gen, die die Etablierung unspezifischer „Nicht-Orte“ (Augé 2012) objektiv zum Ziel hat.

Die folgende Übersicht kontrastiert die beiden unterschiedenen Idealtypen zu Überblickszwecken stichwortartig:

Exkludierend-disziplinierender Idealtypus von Sicherheitspraktiken	**Liberal-inkludierender Idealtypus von Sicherheitspraktiken**
Exklusion (Ausschließung)	Inklusion (Einbeziehung)
Direkt	Indirekt
Sichtbar	Unsichtbar
Normativ aufgeladen	„Management des empirisch Normalen“
Externe Kontrolle, zwangsförmig, oktroyiert	Subjektivierung, interne Kontrolle, Selbstregierung, Responsibilisierung
Körperzentriert	Selbstzentriert
Negative Stigmatisierung	Normalisierung
Produktion exklusiver, regulierter Räume	Produktion von Nicht-Orten

Tabelle 1: Übersicht über die zwei Idealtypen von Sicherheitspraktiken
Eigene Darstellung

4. Modi des Vertrauens

Die unterschiedenen Typen von Sicherheitspraktiken haben nicht nur Bedeutung für die Art und Weise, in der Gefährdungen politisch in den Blick genommen werden, sondern sie zeitigen ebenso markante Implikationen in sozialintegrativer Hinsicht. Um die Frage der (Neben-)Folgen von Sicherheitspraktiken zu fokussieren, soll nachfolgend der Blick auf das Phänomen des Vertrauens gerichtet werden. Dabei wird für eine differenzierte Analyse des Vertrauensphänomens ein modaler Zugriff gewählt, d.h. im Unterschied zu den in der aktuellen Diskussion geläufigen Differenzierungen des Vertrauensbegriffs nach den sog. „Objekten“ bzw. Bezugspunkten des Vertrauens wird ein Vorschlag unterbreitet, der auf die Art und Weise, auf die Ausprägungsform des Vertrauens zielt. In diesem Sinne werden systematisch die Modi eines „reflexiven Vertrauens“, eines „habituellen Vertrauens“ und eines „fungierenden (Grund-)Vertrauens“ unterschieden (vgl. dazu Endreß 2002, 2010a, 2012a, 2013).

Leitend für diesen Differenzierungsvorschlag ist die Annahme, dass Vertrauen im Kern als Hintergrundressource zu verstehen ist, die in ihrem primä-

ren Wirkungsmodus vorrangig implizit und latent bleibt. Vertrauen fungiert alltäglich wesentlich als stillschweigend mitlaufender („vorreflexiv vorausgesetzter") Bezugsrahmen des Welt-, Sozial- und Selbstverhältnisses – und ihm kommt gerade aufgrund dieses vorreflexiven Status seine eminente Wirksamkeit zur Strukturierung sozialer Beziehungen zu. In diesem Sinne soll der Begriff des „fungierenden Vertrauens" der Dimension des „Grundvertrauens" eine für die Soziologie rezipierbare Form geben (vgl. insbesondere Endreß 2002, S. 68ff.; 2010a, S. 97ff., 103ff.; 2013, S. 116ff.). Damit impliziert dieser Begriffsvorschlag zugleich, dass im Kern lediglich für das Grundvertrauen ein fungierender Modus auszumachen ist, weshalb – unter Inkaufnahme einer gewissen Tautologie – durchaus vom fungierenden (Grund-)Vertrauen gesprochen werden kann.

Während also der Modus „fungierenden Vertrauens" verstanden werden soll als der für jedes Welt-, Sozial- und Selbstverhältnis konstitutive (prä-reflexive) Modus von Vertrauen, ist „habituelles Vertrauen" als ebenso prä-reflexives, pragmatisch wirksames Vertrauensfundament der Routinegrundlagen alltäglichen Handelns und Interagierens (und seinerseits als Produkt ebendieser Zusammenhänge) zu begreifen. „Reflexives Vertrauen" schließlich kann verstanden werden als kognitiver Vertrauensmodus und somit als Spezialfall des rational erwogenen Vertrauens im Kontext strategischer Interaktionen. Vertrauen dient hier als kalkuliert einsetzbare Handlungsressource. Reflexives Vertrauen ist deshalb als solches per definitionem thematisch, also explizit und kommunikativ verfügbar. Habituelles Vertrauen hingegen ist lediglich potenziell thematisierbar, also zumindest im Prinzip aus seinem pragmatisch-impliziten Modus bzw. „pragmatischen Schlummer", seiner Latenz, holbar. Fungierendes Vertrauen hingegen ist im Kontrast zu den beiden anderen Vertrauensmodi wesentlich unthematisch und als solches *in praxi* nicht thematisierbar. Fungierendes Vertrauen trägt und begleitet menschliches „Zur-Welt-Sein" (vgl. Merleau-Ponty 1966), menschlichen Weltzugang, d.h. Handeln, Interagieren (intersubjektive Beziehungen) und Verstehen in Gestalt einer notwendig begleitenden, einer unverzichtbaren Hintergrundressource.

5. Verschränkungen von Vertrauensmodi und Typen der Sicherheitsproduktion

Entsprechend der zentralen Bedeutung, die dem Phänomen Vertrauen in seinen unterschiedlichen Modi für Prozesse menschlicher Vergesellschaftung

zugeschrieben werden kann, gehen die nachfolgenden Überlegungen davon aus, dass gesellschaftlich realisierte Formen sozialer Kontrolle bzw. unterschiedliche Formen von Sicherheitspraktiken als Strukturierungsformen von Vergesellschaftungsprozessen in einem ausgeprägten Wechselverhältnis zu gesellschaftlichen „Vertrauenskulturen" stehen. Im Folgenden soll deshalb die Verflechtung der Modi des Vertrauens mit den zuvor herausgearbeiteten Idealtypen von Sicherheitspraktiken untersucht und damit auf (paradoxe) Nebenfolgen der Herstellung von Sicherheit hingewiesen werden. Dabei wird deutlich werden, dass nicht nur die Effekte auf reflexives und habituelles Vertrauen fokussiert werden müssen, sondern insbesondere Auswirkungen für fungierendes (Grund-)Vertrauen gesellschaftlich in den Blick zu nehmen sind.

5.1 Exkludierend-disziplinierender Idealtypus von Sicherheitspraktiken und seine Bedeutung für habituelles und reflexives Vertrauen

Stellt man die im Vorhergehenden skizzierte spezifische „Logik" der Typen von Sicherheitspraktiken und der Vertrauensmodi in Rechnung, dann sind exkludierende bzw. disziplinierende Formen der Sicherheit, also souveräne und direkte Kontrollpraktiken, von besonderer Bedeutung auf der Ebene habituellen und reflexiven Vertrauens.

Dies ist der Fall, weil exkludierend-disziplinierende Formen der Sicherheitsherstellung manifeste Maßnahmen bzw. Praktiken darstellen, also unmittelbar beobachtbar und thematisierbar sind. Zudem werden sie zumeist von politischen bzw. staatlichen Akteuren bzw. Organisationen durchgeführt. Entsprechend werden und können solche Maßnahmen auch politisch diskutiert und hinsichtlich ihres politischen Sinns kritisch erörtert werden. Folglich stehen Fragen politischen Vertrauens und des Organisationsvertrauens auf der Agenda und sind Gegenstand öffentlicher Kontroversen.[7] Hier geht es dominant jeweils um die Modi des habituellen und reflexiven Vertrauens in die Handlungsfähigkeit und den Gestaltungswillen politischer Akteure und das Vertrauen in gesellschaftliche und politische Organisationen.

7 Beispiele für entsprechende Debatten wären u.a. der Sympathisantendiskurs, der seinen sozialwissenschaftlichen Widerhall unter dem Stichwort „Terrorismus und Gesellschaftskritik" fand (vgl. Wellmer 1979), die Debatte um „New Culture", „Old Culture" und „Popular Culture" (vgl. Bohrer 1979), oder die Diskussionen um das Prinzip der „Toleranz" als Ordnungskonzept sog. pluralistischer Massengesellschaften (vgl. Preuß 1979).

Gleichwohl spielt auch in diesem Kontext der Modus fungierenden Vertrauens eine Rolle: Das wird unmittelbar bspw. deutlich, wenn man sich auf den sowohl körperbezogenen wie zwangsförmigen Charakter entsprechender Sicherheitspraktiken mit Blick auf deren Wirkung für einzelne Akteure konzentriert. Individuelle Traumatisierungen als Infragestellung fungierenden (Grund-)Vertrauens sind somit als „Nebeneffekte" exkludierend-disziplinierender Sicherheitspraktiken ebenso in Rechnung zu stellen (vgl. Endreß/ Pabst 2013).

5.2 Liberal-inkludierender Idealtypus von Sicherheitspraktiken und seine Bedeutung für fungierendes Vertrauen

Im Gegensatz dazu lassen sich liberal-inkludierende Formen von Sicherheitspraktiken, d.h. die subtileren, indirekten Selbsttechnologien, die auf die „Logik" der Selbstverantwortlichkeit und der „Regierung aus der Distanz" abstellen, deutlich schwieriger in ihren Effekten für eine gesellschaftliche Vertrauenskultur thematisieren und analysieren.

Nichtsdestoweniger haben sie gerade aufgrund ihres indirekten, mittelbaren Charakters starke Effekte auf Vertrauensverhältnisse, genauer: auf den Modus fungierenden Vertrauens. Aufruhend auf der Annahme allgegenwärtiger Risiken und eines entsprechend proaktiven Zuschnitts adressieren liberale Sicherheitsmechanismen nicht konkrete Bedrohungen, sondern eben gerade gesellschaftliche Konstellationen in ihrer Gesamtheit. Sie etablieren strukturnotwendig eine Kultur allseitigen Verdachts.

Unter Rekurs auf ein klassisches Argument von Erving Goffman lässt sich deshalb formulieren, dass liberal-inkludierende Praktiken der Sicherheitsproduktion dazu angetan sind, die Kultur der grundlegenden „civil inattention" (der „höflichen Unaufmerksamkeit") des gesellschaftlichen Miteinanders zu destabilisieren, wenn nicht zu untergraben, und im Gegenzug mit dem Imperativ einer allumfassenden „civil attention" den Verdacht bzw. eine proaktive Aufmerksamkeitskultur zum Grundphänomen sozialen Lebens zu erheben. Sozialität mutiert solchermaßen zu einer Sozialität unter Vorbehalt (vgl. Goffman 1971). Und dieser Vorbehalt tangiert ganz offensichtlich den zuvor skizzierten Vergesellschaftungsmodus fungierenden (Grund-)Vertrauens.

Um diesen Zusammenhang in eine stärker politische Sprache zu überführen: Die vorgängige Unschuldsvermutung im wechselseitigen sozialen Verkehr wird brüchig. D.h. wir haben es mit einer grundlegenden Erschütterung des menschlichen Sozial- und Weltverhältnisses zu tun, die notwendig Impli-

kationen für die jeweiligen Selbstverhältnisse von Akteuren nach sich zieht. Fungierendes Vertrauen als alltägliche Hintergrundressource sozialen Lebens wird von einer Dauerressource zu einem Dauerproblem.

Aus diesem Grund lässt sich argumentieren, dass liberal-inkludierende Formen von Sicherheitspraktiken Traumatisierungsprozesse nach sich ziehen (können); aber im Unterschied zu exkludierend-disziplinierenden Formen von Sicherheitspraktiken nicht nur und vorrangig auf individueller Ebene, sondern darüber hinausgehend gerade auf sozialer, respektive gesellschaftlicher und politischer Ebene in Form von um sich greifenden Verunsicherungsgefühlen und Bedrohungsphantasien. Damit sind Konstellationen angesprochen, die durchaus mit den Konzepten „cultural trauma" oder auch „collective trauma" gefasst werden können, womit Anschluss an eine weitere aktuelle Diskussion der Soziologie gewonnen wäre (vgl. u.a. Alexander et al. 2004).

Mit dieser Diagnose schließt sich dann in gewisser Hinsicht der Kreis, insofern hier Phänomenkonturen erneut in den Blick treten, die aus den eingangs erwähnten Diskussionszusammenhängen unter den Stichworten der Flexibilisierung und des flexiblen Selbst in der sogenannten „Spätmoderne" bekannt sind und eingeführt wurden.

6. Resümee

Ziel der vorliegenden Ausführungen war es, Idealtypen von Sicherheitspraktiken in der Gegenwartsgesellschaft zu unterscheiden und diese in ihren Konsequenzen an die Analyse von gesellschaftlichen Vertrauenskulturen rückzubinden. Gegenwartsgesellschaften werden durch die Vorstellung grundlegender Unsicherheiten, allumfassender Risiken und das Konzept der Sicherheit als zentralem Wertbegriff maßgeblich bestimmt. In diesem Kontext werden „klassische" Formen exkludierend-disziplinierender Sicherheitsproduktion zumindest ergänzt, wenn nicht überwölbt von liberal-inkludierenden Formen von Sicherheitspraktiken, deren Augenmerk auf der Responsibilisierung und Selbstführung von Individuen liegt. Um die Folgen dieses Wandels zu charakterisieren, wurde auf eine Unterscheidung von Vertrauensmodi zurückgegriffen und wurden insbesondere die Effekte auf den Modus fungierenden Vertrauens und damit auf die Erosion gesellschaftlicher Vertrauenskulturen generell herausgestellt. Damit wurde im Kern auf die paradoxen Effekte aktueller Formen von Sicherheitspraktiken hingewiesen.

Literatur

Agamben, G. (2004): Ausnahmezustand. Frankfurt am Main

Alexander, J. C.; Eyerman, R.; Giesen, B.; Smelser, N. J.; Sztompka, P. (2004): Cultural Trauma and Collective Identity. Berkeley

Augé, M. (2012): Nicht-Orte. München

Balzacq, T. (Hg.) (2011): Securitization Theory. How Security Problems Emerge and Dissolve. London/New York

Baudrillard, J. (1983): Simulations. New York

Bauman, Z. (2003): Flüchtige Moderne. Frankfurt am Main

Beck, U. (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main

Beck, U. (1993): Die Erfindung des Politischen. Zu einer Theorie reflexiver Modernisierung. Frankfurt am Main

Beck, U.; Giddens, A.; Lash, S. (1996): Reflexive Modernisierung. Eine Kontroverse. Frankfurt am Main

Böschen, S.; Kratzer, N.; May, S. (Hg.) (2006): Nebenfolgen. Analysen zur Konstruktion und Transformation moderner Gesellschaften. Weilerswist

Bohrer, K. H. (1979): Die drei Kulturen. In: Habermas, J. (Hg.): Stichworte zur „Geistigen Situation der Zeit". Frankfurt am Main, S. 636-669

Daase, C. (2002): Internationale Risikopolitik. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel. In: Daase, C.; Feske, S.; Peters, I. (Hg.): Internationale Risikopolitik. Der Umgang mit neuen Gefahren in den internationalen Beziehungen. Baden-Baden, S. 9-35

Daase, C. (2010a): Der erweiterte Sicherheitsbegriff. Working Paper 1/2010 des Projekts „Sicherheitskultur im Wandel". – URL: http://www.sicherheitskultur.org/WorkingPapers/01-Daase.pdf [30.05.2012]

Daase, Christopher (2010b): Wandel der Sicherheitskultur. In: Aus Politik und Zeitgeschichte, H. 50, S. 9-16

Deleuze, G. (1993): Postskriptum über die Kontrollgesellschaften. In: Deleuze, G.: Unterhandlungen 1972-1990. Frankfurt am Main, S. 254-262

Elias, N. (1969): Über den Prozess der Zivilisation. Soziogenetische und psychogenetische Untersuchungen, 2 Bde. Bern/München

Endreß, M. (2002): Vertrauen. Bielefeld

Endreß, M. (2004): Foundations of Trust. Introductory Remarks on the Sociology of Trust. In: Schrader, H. (ed.): Trust and Social Transformation. Theoretical Approaches and Empirical Findings from Russia. Münster, pp. 15-30

Endreß, M. (2010a): Vertrauen – soziologische Perspektiven. In: Maring, M. (Hg.): Vertrauen – zwischen sozialem Kitt und der Senkung von Transaktionskosten. Karlsruhe, S. 91-113

Endreß, M. (2010b): Vertrauenskrisen und Vertrauensverluste. In: Widerspruch. Münchner Zeitschrift für Philosophie, H. 51, S. 27-40

Endreß, M. (2010c): Unvorhergesehene Effekte – altes Thema, neue Probleme? In: Albert, G.; Greshoff, R.; Schützeichel, R. (Hg.): Dimensionen und Konzeptionen von Sozialität. Wiesbaden, S. 13-32

Endreß, M. (2012a): Vertrauen und Misstrauen – Soziologische Überlegungen. In: Schilcher, C.; Will-Zocholl, M.; Ziegler, M. (Hg.): Vertrauen und Kooperation in der Arbeitswelt. Wiesbaden, S. 81-102

Endreß, M. (2012b): Trust and the Dialectic of the Familiar and the Unfamiliar within the Life-World. In: Nasu, H.; Waksler, F. C. (eds.): Interaction and Everyday Life. Phenomenological and Ethnomethodological Essays in Honor of George Psathas. Lanham, pp. 115-133

Endreß, M. (2013): Zur Struktur von „Grundvertrauen" und der Vertrauenssignatur in Gegenwartsgesellschaften. In: Dalferth, I. U.; Preng-Keller, S. (Hg.): Grundvertrauen. Hermeneutik eines Grenzphänomens. Leipzig, S. 115-144

Endreß, M.; Pabst, A. (2013): Violence and Shattered Trust – Sociological Considerations. In: Human Studies, Vol. 36, No. 1, pp. 89-106

Foucault, M. (1977): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main

Foucault, M. (1999): In Verteidigung der Gesellschaft. Vorlesungen am Collège de France (1975-1976). Frankfurt am Main

Foucault, M. (2005): „Omnes et singulatim": Zu einer Kritik der politischen Vernunft. In: Foucault, M.: Dits et Ecrits. Schriften in vier Bänden. Band IV: 1980-1988. Frankfurt am Main, S. 165-198

Foucault, M.. (2006a): Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I. Vorlesung am Collège de France 1977-1978. Frankfurt am Main

Foucault, M. (2006b): Die Geburt der Biopolitik. Geschichte der Gouvernementalität II. Vorlesung am Collège de France 1977-1978. Frankfurt am Main

Foucault, M. (2009): Hermeneutik des Subjekts. Vorlesungen am Collège de France 1981-1982. Frankfurt am Main

Garland, D. (2008): Kultur der Kontrolle. Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Frankfurt am Main (Frankfurter Beiträge zur Soziologie und Sozialphilosophie)

Goffman, E. (1971): Relations in Public. Microstudies of the Public Order. New York

Groenemeyer, A. (Hg.) (2010): Wege der Sicherheitsgesellschaft. Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten. Wiesbaden

Gross, P. (1994): Die Multioptionsgesellschaft. Frankfurt am Main

Kaufmann, F.-X. (1973): Sicherheit als soziologisches und sozialpolitisches Problem. Untersuchungen zu einer Wertidee hochdifferenzierter Gesellschaften. 2. umgearb. Aufl. Stuttgart

Krasmann, S. (2003): Die Kriminalität der Gesellschaft. Zur Gouvernementalität der Gegenwart. Konstanz

Legnaro, A. (1997): Konturen der Sicherheitsgesellschaft: Eine polemisch-futurologische Skizze. In: Leviathan, Jg. 25, H. 2, S. 271-284

Lemke, T. (1997): Eine Kritik der politischen Vernunft. Foucaults Analyse der modernen Gouvernementalität. Hamburg

Merleau-Ponty, M. (1966): Phänomenologie der Wahrnehmung. Berlin

Neckel, S.; Sutterlüty, F. (2005): Negative Klassifikationen. Konflikte um die symbolische Ordnung sozialer Ungleichheit. In: Heitmeyer, W.; Imbusch, P. (Hg.): Integrationspotenziale einer modernen Gesellschaft. Analysen zu gesellschaftlicher Integration und Desintegration. Wiesbaden, S. 409-428

Paris, R. (2001): Human Security. Paradigm Shift or Hot Air? In: International Security, Vol. 26, No. 2, pp. 87-102

Preuß, U. K. (1979): Politische Ordnungskonzepte für die Massengesellschaft. In: Habermas, J. (Hg.): Stichworte zur „Geistigen Situation der Zeit". Frankfurt am Main, S. 340-378

Schmitt, C. (1993): Politische Theologie. Vier Kapitel zur Lehre von der Souveränität [1922/1928]. 6. Aufl. Berlin

Schneckener, U. (2006): Transnationaler Terrorismus. Charakter und Hintergründe des „neuen" Terrorismus. Frankfurt am Main

Schulze, G. (1992): Die Erlebnisgesellschaft. Kultursoziologie der Gegenwart. Frankfurt am Main/New York

Sennett, R. (1998): Der flexible Mensch. Die Kultur des neuen Kapitalismus. Berlin

Sennett, R. (2007): Die Kultur des neuen Kapitalismus. Berlin

Singelnstein, T.; Stolle, P. (2012): Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert. 3. überarb. u. erg. Aufl. Wiesbaden

Wacquant, L. (2009): Bestrafen der Armen. Zur neoliberalen Regierung der sozialen Unsicherheit. Opladen/Farmington Hills

Wæver, O. (1995): Securitization and Desecuritization. In: Lipschutz, R. (ed.): On Security. New York, pp. 46-86

Wellmer, A. (1979): Terrorismus und Gesellschaftskritik. In: Habermas, J. (Hg.): Stichworte zur „Geistigen Situation der Zeit". Frankfurt am Main, S. 265-293

Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 161–163*

Ernst-Otto Reher, Gerhard Banse

Schlusswort

Am Ende dieses interessanten Symposium muss zunächst gefragt werden, ob das geplante Ziel erreicht worden ist, das im Symposiumsmaterial folgendermaßen formuliert worden war: „In dem geplanten eintägigen Symposium werden Wissenschaftler aus verschiedenen Disziplinen ihre Forschungsergebnisse zum Thema (Technik-)Sicherheit mit dem Ziel diskutieren, gemeinsame Forschungsansätze vor allem zu Techniksicherheit, aber auch zu Sicherheitskommunikation und Sicherheitskulturen zu entwickeln.“ Elf Vorträge aus unterschiedlichen Gebieten der Technikwissenschaften, aus der Soziologie, aus der Linguistik und aus der Philosophie sowie eine intensive Diskussion belegen, dass das gewählte Thema facettenreich und interdisziplinär erörtert, das Ziel somit erreicht worden ist. Deshalb gilt der Dank allen Vortragenden und Diskutanten. Das Thema „Sicherheit“ ist es wert, auch außerhalb der Leibniz-Sozietät fächerübergreifend behandelt zu werden (z.B. im Rahmen der berlin-brandenburgischen Sicherheitswirtschaft).

Sodann soll eine kurze Bilanz der bisherigen Tätigkeit des Arbeitskreises „Allgemeine Technologie“ gezogen und auf weitere Vorhaben aufmerksam gemacht werden:[1]

1. Der Arbeitskreis „Allgemeine Technologie“ hat bisher fünf Symposien organisiert und gestaltet (in den Jahren 2001, 2004, 2007, 2010 und 2012; die Ergebnisse wurden in den Bänden 50, 75, 99 und 112 der „Sitzungsberichte der Leibniz-Sozietät“ publiziert). Drei Symposien behandelten Grundlagen und zwei Symposien behandelten verschiedene weitergehende Facetten der Allgemeinen Technologie (Ambivalenzen, Sicherheit). Es sollte an einer zweijährigen Fortsetzung (2014, 2016, …) festgehalten werden, um weitere aktuelle Probleme der Allgemeinen Technologie interdisziplinär erörtern zu können.

1 Vgl. auch http://leibnizsozietaet.de/sozietaet/arbeitskreise/.

2. Mitglieder des Arbeitskreises haben sich darüber hinaus in den Jahrestagungen der Leibniz-Sozietät und in Veranstaltungen des LIFIS – Leibniz-Institut für interdisziplinäre Studien – geäußert sowie Beiträge in den „Abhandlungen der Leibniz-Sozietät" publiziert. Ein eigenständiger Band in dieser Reihe mit dem Arbeitsthema „Beiträge zur Allgemeinen Technologie" ist in der Erarbeitung. Angestrebt wird, eine „Enzyklopädie Allgemeine Technologie" zu verfassen, eventuell gemeinsam mit der Deutschen Akademie der Technikwissenschaften (acatech).
3. Vorschläge für mögliche weitere Symposien des Arbeitskreises sind:
   – Technologiewandel in der Wissensgesellschaft.
   – Nachhaltige Ressourcenbereitstellung (Rohstoffe und Technologien) für Wachstum und soziale Gerechtigkeit.
   – Was liefern die Erzeugnis- und Vorgangstechnologien an Voraussetzungen für die Konstituierung der Allgemeinen Technologie?
4. Sinnvoll ist die Erarbeitung einer Konzeption für eine (interdisziplinäre) Lehrveranstaltung (Vorlesung und/oder Seminar) „Allgemeine Technologie" und ihre Empfehlung bzw. Erprobung an wissenschaftlichen Bildungsstätten (Universitäten, Hoch- und Fachschulen). Da u.a. an den Universitäten in Cottbus und Potsdam Erfahrungen mit derartigen Lehrveranstaltungen vorliegen, sollte eine kleine Arbeitsgruppe diese Ausarbeitung vornehmen, die dann anderen Bildungsstätten empfohlen werden kann.[2]

   Neben dem unmittelbaren Wissenstransfer könnten weitergehende Ziele dieser Lehrveranstaltung sein:
   – Grundständige „Einbettung" der Lehrveranstaltung im Rahmen des „Studium generale" in den Anfangssemestern.
   – Behandlung allgemeiner technologischer Prinzipien, Gesetze, Methoden, Algorithmen, Verfahren, Restriktionen usw., die ihre Vertiefungen und Konkretisierungen in den speziellen (Erzeugnis-)Technologien der Bildungsstätte (z.B. Chemische Technologie, Pharmazeutische Tech-

2 Das ist zwischenzeitlich erfolgt: Im Sommersemester 2013 wird durch Gerhard Banse, MLS (Berlin), Wolfgang Fratzscher (Halle/Saale), Klaus Krug, MLS (Merseburg) und Ernst-Otto Reher, MLS (Halle/Saale) an der Hochschule Merseburg die Lehrveranstaltung „Einführung in die Allgemeine Technologie – Umriss einer Theorie der Technik –" im Umfang von 2 Semesterwochenstunden erfolgreich durchgeführt. – Diese in Form von Vorlesungen durchgeführte Lehrveranstaltung wird von der Hochschule Merseburg in Wort und Bild aufgezeichnet, um daraus unter Einbeziehung der verwendeten Präsentationen ein Lehrmaterial zu erstellen.

nologie, Biotechnologie, Nanotechnologie, Kunststoff- und Werkstofftechnologie u.ä.) finden.
- Schaffung einer interdisziplinären Plattform, auf der Vertreter der Naturwissenschaften, der Technikwissenschaften und der Sozial- und Geisteswissenschaften gemeinsame Projekte entwickeln können.

Mit diesen wenigen Anmerkungen zu Ergebnissen wie zu Programmatischem wird u.E. deutlich, dass der Arbeitskreis „Allgemeine Technologie“ der Leibniz-Sozietät seine Berechtigung wie seine Leistungsfähigkeit unter Beweis gestellt hat und das auch weiterhin tun wird.